# INFORMATION ASSURANCE AND THE DEFENSE IN DEPTH: A STUDY OF INFOSEC WARRIORS AND INFOSEC COWBOYS

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

JONATHAN M. FOX, MAJ, USA
B.S., United States Military Academy, West Point, New York, 1991
M.S., American Intercontinental University, Los Angeles, California, 2000

Fort Leavenworth, Kansas
2003

# REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188



| 1. REPORT DATE (DD-MM-YYYY) | 2. REPORT TYPE | 3. DATES COVERED (FROM - TO) |
|---|---|---|
| 06-06-2003 | thesis | 05-08-2002 to 06-06-2003 |

4. TITLE AND SUBTITLE
INFORMATION ASSURANCE AND THE DEFENSE IN DEPTH:
A STUDY OF INFOSEC WARRIORS AND INFOSEC COWBOYS
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Fox, Jonathan, M

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
US Army Command and General Staff College
1 Reynolds Ave
Fort Leavenworth, KS66027-1352

8. PERFORMING ORGANIZATION REPORT NUMBER
ATZL-SWD-GD

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
A1,Administrative or Operational Use
06-06-2003
US Army Command and General Staff College
1 Reynolds Ave
Ft. Leavenworth, KS66027-1352

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This study investigates the Army?s ability to provide information assurance for the NIPRNET. Information assurance includes those actions that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. The study examines how the military?s defense in depth policy provides information assurance with a system of layered network defenses. The study also examines current practices used in the corporate world to provide information assurance. With the cooperation of the Human Firewall Council, the study compared the performance of four organizations according to standards developed for the Council?s Security Management Index. The four participants in the study included: an Army Directorate of Information Management, a government agency, a university, and a web development company. The study also compared the performance of the four participants with the aggregate results obtained by the Human Firewall Council. The study concluded the defense in depth policy does grant the Army an advantage over other organizations for providing information assurance. However, the Army would benefit from incorporating some of the common practices of private corporations in their overall information assurance plans.

15. SUBJECT TERMS
Army; NIPRNET; Information assurance; Security; Defense

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| | | | Same as Report (SAR) | 160 | Buker, Kathy<br>kathy.buker@us.army.mil |
| a. REPORT<br>Unclassified | b. ABSTRACT<br>Unclassified | c. THIS PAGE<br>Unclassified | | | 19b. TELEPHONE NUMBER<br>International Area Code<br>Area Code Telephone Number<br>9137583138<br>DSN<br>5853138 |

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Jonathan M. Fox

Thesis Title: Information Assurance and the Defense in Depth: A Study of Infosec Warriors and Infosec Cowboys

Approved by:

_____, Thesis Committee Chairman
LtCol Richard W. Snyder, M.A.

_____, Member
LCDR Bob A. King, M.A.

_____, Member, Consulting Faculty
LTC Kenneth D. Plowman, Ph.D.

Accepted this 6th day of June 2003 by:

_____, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

INFORMATION ASSURANCE AND THE DEFENSE IN DEPTH: A STUDY OF INFOSEC WARRIORS AND INFOSEC COWBOYS by MAJ Jonathan Fox, USA, 151 pages.

This study investigates the Army's ability to provide information assurance for the NIPRNET. Information assurance includes those actions that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation.

The study examines how the military's defense in depth policy provides information assurance with a system of layered network defenses. The study also examines current practices used in the corporate world to provide information assurance.

With the cooperation of the Human Firewall Council, the study compared the performance of four organizations according to standards developed for the Council's Security Management Index. The four participants in the study included: an Army Directorate of Information Management, a government agency, a university, and a web development company. The study also compared the performance of the four participants with the aggregate results obtained by the Human Firewall Council.

The study concluded the defense in depth policy does grant the Army an advantage over other organizations for providing information assurance. However, the Army would benefit from incorporating some of the common practices of private corporations in their overall information assurance plans.

ACKNOWLEDGMENTS

The author would like to thank the survey participants for their time and assistance in the conduct of this research. Though anonymous in this report, your support and your efforts to provide a higher level of information assurance for us all are appreciated. A special thank you goes to Mister Todd Tucker at NetIQ and Mister John Ortbal, the Director of the Human Firewall Council. Their permission to use the Security Management Index was critical to the success of this research, and I hope it helps make us all “more aware and more secure.”

TABLE OF CONTENTS

ILLUSTRATIONS

TABLES

# CHAPTER 1

## INTRODUCTION

In October 1969, the first login session of the ARPANET occurred between the University of California, Los Angeles (UCLA) and the Stanford Research Institute (SRI). At UCLA, an undergraduate student named Charlie Kline typed the letters L-O-G on his computer while another researcher at SRI read the code on his screen. This exchange of data across a computer network was the foundation of today's Internet. It was also the foundation for information assurance. For though the scientists can explain packet switching and assembly language, even today they cannot answer the question of "who was the researcher at SRI?" (Hafner and Lyon 1996, 153). The question of who was responding from SRI might not be significant to the historian but it is significant to the network managers of today. Today network managers are asking questions related to information assurance: How do I authenticate users? How do I ensure confidentiality? How do I ensure data integrity? The questions asked today surrounding information assurance were introduced at the first login in 1969: Will this network always be available? Who am I really communicating with? Can anyone else read my message? Is the text I read on the screen really what the other person sent? How do we track who communicates what, with who, and when? These questions are critically important in today's military.

The American military today is the most networked force in the world. The vision of the transformed armed forces places an even higher effort on obtaining information superiority, the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (Joint Pub

3-13 1998, GL-7). Though our armed forces are most capable of obtaining information superiority, we are also most vulnerable to attacks on our systems and our information. In order to protect our systems and information, the Joint military community uses a Defense in Depth approach to provide information assurance (Joint Staff Publication 2000, 3).

What is information assurance? As defined in Joint Pub 3-13, information assurance is a subset of information operations. Information operations (IO) are operations conducted to defend our own information and information systems and affect adversary information and information systems. Information assurance includes those actions "that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" (Joint Pub 3-13 1998, GL-7).

## Significance of Study

Why is information assurance important to the unclassified IT systems of the Department of Defense? As pointed out in *Grand Strategy for Information Age National Security*, the United States is most vulnerable to Information Warfare for three reasons. First, the United States is the most information dependent country in the world. The United States military, economy, and culture are all dependent on information. Lieutenant Colonel Kevin Kennedy, author of the *Grand Strategy for Information Age National Security*, described the United States as the "most wired" country. Second, as the most dependent country on information, the United States is also the most vulnerable country

to information attacks. Third, the same technology the United States uses to share information can be used by adversaries to impact on the political and cultural fabric of the American society (Kennedy, Lawlor, and Nelson 1997, 2). Robert Dunlap, in his essay "How We Lost the War of 2007," painted an ominous view of American susceptibility to information operations. The adversary in Dunlap's essay is able to use the media and the Internet to distort truth about a nuclear explosion (Dunlap 1996). Information assurance efforts must protect the integrity of data being reported and broadcast.

## Defense in Depth

How does the Defense in Depth approach provide for information assurance? In 1999, Chaos Communications sponsored a competition in Germany called the Linux Death Match. The challenge was for teams of network administrators and hackers to knock out each other's network services. The winning team did not have a great attack plan. In fact, they did not have an attack plan. They simply installed as much security software as they could download (Hayes 1999). After seeing the results of the Linux Death Match, the military followed the example of the successful network administrators by focusing on defense and lots of it.

The Defense in Depth approach focuses the defense through three main efforts: people, operations, and technology. The intent of Defense in Depth is "to establish multi-layer, multi-dimension protection" (Joint Staff Publication 2000, 6). Similar to a physical defense, the Defense in Depth depends on redundancy and risk analysis to ensure that forces are applied at the right time and the right place.

The first forces applied through Defense in Depth are people. People are the core component of the Defense in Depth approach. From the user to the network administrator, people are ultimately the power behind the technology. The Defense in Depth approach stresses the importance of educating, training, certifying, and retaining the best personnel for key security roles (Joint Staff Publication 2000, 7). Jay Lyman, of NewsFactor, outlined the profile of the perfect security guru:

> They know how to set up and maintain firewall, antivirus and intrusion detection systems. They know how to scan the company network for holes. They are up to speed on the latest vulnerabilities and know whether or not software patches are available. They know what to do when the corporate servers get hacked, and they know how to stop the attack in its tracks. They also have the gumption to tell you when they cannot handle something, and they can recommend where to go for help. (Lyman, "Profile of the Perfect Security Guru," 2002)

The second forces applied through the Defense in Depth Approach are the operations. Operations are driven by policies that relate to information assurance. Three main levels of operations help focus users and administrators: program policies, issue-specific policies, and system-specific policies. Organizations establish *program policies* that define the local requirements of security in terms of purpose, goals, scope, resource allocation, authorities, responsibilities, and compliance. Specific issues related to system use can be addressed by *issue-specific policies*. Finally, a *system-specific policy* can address usage standards and procedural rules for specific systems (Joint Staff Publication 2000, 8).

Technology is the final force applied in the Defense in Depth approach. Technology provides the weapons required to conduct an active defense. Several key areas where technology plays an important role include redundant data paths, intrusion

detection, cryptography, firewalls, identification, and authorization (Joint Staff Publication 2000, 11).

This thesis will attempt to determine if the Defense in Depth approach provides United States Army IT professionals with an advantage over their civilian counterparts for providing information assurance for the NIPRNET. The primary comparison will be between the military unclassified systems with similar corporate systems. The metrics used for comparison will be the Security Management Index developed by the Human Firewall Council, an organization of information security professionals focused on educating the public of the human and technical issues involved in information security. Based on the standards established by ISO 17799, the Security Management Index offers a benchmark of security management practices among survey participants. Developed by the British Standards Institute, ISO 17799 offers the only international standards for information security (Human Firewall 2002). The Security Management Index measures an organization's approach for providing information assurance in the following ten areas:

1) Security Policy
2) Organization of assets and resources
3) Asset classification and control
4) Personnel security
5) Physical and environmental security
6) Communications and operations management
7) Access control
8) Systems development and maintenance
9) Business continuity management
10) Compliance

## Terms and Definitions

The Defense in Depth approach establishes the following criteria, as defined in the Joint Publication, *Information Assurance through Defense in Depth*:

Availability: Timely, reliable access to data and services for authorized users. The attribute of availability includes restoration (Joint Staff Publication 2000, 2). What percentage of the time will this network be available to the users?

Identification and Authentication: Identification is the process an information system uses to recognize an entity. Authentication is a security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an authorization to receive specific categories of information (Joint Staff Publication 2000, 2). Who am I really communicating with?

Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices (Joint Staff Publication 2000, 2). Can anyone else read my message?

Integrity: Protection against unauthorized modification or destruction of information (Joint Staff Publication 2000, 2). Is the text I read on the screen really what the other person sent?

Nonrepudiation: The sender is provided with proof of delivery, and the recipient is provided with proof of the sender's identity, so neither can deny having processed the data (Joint Staff Publication 2000, 2). How do we track who communicates what, with who, and when?

Other terms used throughout this thesis are also defined in various military publications:

Information Assurance: Information assurance is a subset of information operations. Information assurance includes those actions “that protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation.” This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (Joint Pub 3-13 1998, GL-7).

Information Operations: Information operations are operations conducted to defend our own information and information systems and affect adversary information and information systems (Joint Pub 3-13 1998, GL-7).

Local Computing Environment (Enclave): The total physical and organizational environment, including all end-system devices and communication systems (such as relay systems) under control of a single authority with a common, uniform policy that governs security related practices. Includes data, applications, people, and facilities (Joint Staff Publication 2000, 4).

Networks: Networks to transport data and information between enclaves. Includes data, applications, people, and facilities (Joint Staff Publication 2000, 4).

Supporting Infrastructures: Organized capabilities to provide special support, such as cryptographic logistics (Joint Staff Publication 2000, 4).

This study also uses several term related to the Human Firewall Security Management Index and information security in general. These terms are defined on the Human Firewall website and by various other information security publications.

Security Policy: The development of policy that provides the managerial direction and support for information security (Human Firewall 2002).

Organizational Security: The policies and actions taken within an organization to provide for and manage information security (BSI Management 2002).

Asset Classification and Control: The ability of organization to identify and classify data and information systems according to the value assigned for protecting them (BSI Management 2002).

Personnel Security: The actions taken within an organization to reduce the risk of insider error or misuse (Human Firewall 2002).

Physical and Environmental Security: The policies and actions that examines the threats and countermeasures required to physically protect an organization's information systems and other resources (Miller and Gregory 2002, 22).

Communications and Operations Management: The domain that covers all the actions and policies taken to ensure protection is provided for all information processing regardless of transmission medium (Miller and Gregory 2002, 18).

Access Control: The steps taken to limit access to information or information systems within an organization. Includes both technical and non-technical controls (Boyce and Jennings 2002, 17).

Systems Development and Maintenance: The process by which an organization considers and provides for information security during the development of information systems and software (Miller and Gregory 2002, 19).

Business Continuity Management: The actions taken to limit disruptions of normal operations as a result of major system failures or other natural or man-made disasters (BSI Management 2002).

Compliance: The steps incorporated in an organization's information security plan to avoid breaches of any criminal or civil law or other statutory requirement (Human Firewall 2002).

## Conclusion

This thesis is limited to a discussion of unclassified networks and automation systems within the Department of Defense and counterpart civilian systems. Constraints on time and classified processing systems do not support an examination of secure networks such as SIPRNET or the Global Command Control System.

For the purpose of time and scope, the standardized interviews conducted for the research of this thesis will be constrained to a sampling of the population within corporate industries. The study will include representatives from commercial computer consultants and solution providers and a state level university. On the military side, an installation Directorate of Information Management (DOIM) will be used as the sample for the Army networks. Finally, a government agency outside the military will be used as a sample for comparison of information assurance performance within the United States government.

The remaining chapters of this thesis attempt to answer the question of does the Defense in Depth policy provide the Army IT professionals with an advantage over their civilian counterparts. Chapter 2 reviews the current literature available on the military's, the government's, and the corporate world's view of information assurance: what is information assurance; how does an organization provide for information assurance; and finally why is information assurance important? Chapter 3 introduces the Security

Management Index developed by the Human Firewall Council. This study will use the Security Management Index to survey the four participants and to determine their SMI score. Chapter 4 reviews the survey results and compares the performance of the four survey participants with the over 1000 respondents to the Human Firewall Council's Security Management Index. Finally, Chapter 5 discusses the findings, examines the road ahead, and makes recommendations for further research.

# CHAPTER 2

# LITERATURE REVIEW

Ever since the proliferation of the World Wide Web and the Internet, much has been written and said with regards to information security, and lately to information assurance. A review of the available literature offers this study an opportunity to answer several of the secondary research questions: How does the Army and the rest of the military define information assurance? How does the military provide information assurance? How do other government agencies define and provide information assurance? What do those outside of the military and government think of information assurance? What general principles do civilians apply in order to provide information assurance? Why is information assurance important?

## The Military and Information Assurance

In 1996, the Army produced their first doctrinal manual for dealing with information and information sources: FM 100-6 *Information Operations*. FM 100-6 outlined the importance of information to the commander's ability to synchronize combat functions on the battlefield. While the manual does not use the term "information assurance", FM 100-6 does introduce information security as the protection of information and the denial of information to unauthorized users (FM 100-6 1996).

The Joint Staff followed the Army only one year later with the publication of Joint Pub 3-13, *Joint Doctrine for Information Operations* in 1998. This publication introduced the term "information assurance" and provided the definition used in this study. Information assurance includes those actions "that protect and defend information

and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation" (Joint Pub 3-13 1998, GL-7).

By the year 2000, the Joint Staff and the Department of Defense began to issue both policy and implementation guidance for providing information assurance. In 2000, the Joint Staff presented their first publication focused exclusively for those personnel involved with computer and computer network defense with *Information Assurance through Defense in Depth*. This publication provided network administrators and their commanders with a simple explanation of the Defense in Depth policy and how information assurance helps provide the warfighter with correct information at the appropriate time (Joint Staff Publication 2000, 1-2).

For policy guidance, the Chief Information Officer published Department of Defense Policy Memorandum No. 6-8510, "Department of Defense Global Information Grid Information Assurance. This policy outlined the specific responsibilities of commanders and their staffs must take to provide the information assurance needs of the warfighter and the daily business military (U.S Department of Defense 2000, 3).

The Army followed in March of 1998 by providing policy and regulatory guidance with the publication of Army Regulation 380-19, *Information Systems Security.* AR 380-19 introduced the concept of site accreditation for information systems processing. In addition, AR 380-19 attempted to adapt to the changing environment with guidance on laptop computers usage, Internet usage, and computer and communications security (AR 380-19 1998, i).

The publication of Army Regulation 380-5, *Department of the Army Information Security Program* in September of 2000 further outlined policy and regulatory guidance

for the Army. AR 380-5 provides the overview of information security, classification, and access control in relation to security classification (AR 380-5 2000, i).

To supplement the regulatory guidance, the academic side of the military produced a continuous flow of theses and essays on the subject of information assurance. The National War College and the Service Colleges have provided this outlet for research and writings on information assurance.

Most of the military research deals with the question of why is information assurance important. The Air University Press released *Grand Strategy for Information Age National Security* back in 1997. As discussed in Chapter 1, *Grand Strategy* outlined why the United States is most vulnerable to information warfare and proposes, "information assurance should be the theme for US defensive grand strategy" (Kennedy, Lawlor, and Nelson 1997, ix). The War College followed with *Five-Dimensional (Cyber) Warfighting* in 1998. In a vein similar to Dunlap's "How we lost the war of 2007", Robert Bunker described how the Army forces of the future can be defeated by an enemy that denies the United States information superiority (Bunker 1998, 27). Both of these publications provide a unique perspective on why the military must be concerned with information assurance.

As part of providing information assurance, IT professionals must be concerned with the capabilities and motivations of the threat. The Air Force Institute of Technology published research on that compared taxonomies used by military and civilian IT personnel. "Analysis of the Computer and Network Attack Taxonomy" provided a basic review of the language of network attacks and their impact on Air Force operations

(Daigle 2001, 66). Understanding the threat and the models used to analyze attacks assists IT professionals in their efforts to provide information assurance.

In an effort to examine the question of how could the military improve their ability to provide for information assurance, the Naval Postgraduate School sponsored the work "Network Defense-in-Depth: Evaluating Host-Based Intrusion Detection Systems." This research project outlined the basics of layer one protection with intrusion detection systems. The work reviewed the defense in depth concept and looked at the technological solutions provided by host-based, off the shelf, intrusion detection systems (Yun and Vozzola 2001, v).

But how does the military provide information assurance? At a recent information security conference, U.S. Marine Lieutenant Colonel Rob Ashworth, Information Assurance Branch Chief for Central Command (CENTCOM), outlined how the Defense in Depth policy is implemented at the combatant commander level. LtCol Ashworth employs Defense in Depth by focusing on people, tools, procedures, and policies. The method used by CENTCOM splits the operations layer of the Defense in Depth policy into procedures and policies. This split helps provide adjustable layers of defense whether operating in garrison or from a forward deployed location (Ashworth 2003).

## The Government and Information Assurance

How do other government agencies outside the military view information assurance? The research efforts of the government produced the Information Assurance Technical Framework (IATF). The IATF is sponsored by the National Security Agency (NSA) and is the standard for technical guidance relating to Information Assurance. The

IATF uses the Defense in Depth approach as its "framework" to structure the information provided on the IATF website. Government, military, and other personnel can access, through the Internet, three levels of information: the main body, executive summaries, and protection profiles. The main body provides general guidance while the executive summaries provide more detailed guidance related to specific issues or systems. Finally, the protection profiles offer the specific security requirements related to certain systems or products (National Security Agency 2002).

In September of 2002, the NAS released version 3.1 of the IATF. While the framework is intended to be a fluid document that adjusts to changes in technologies and threats, the doctrinal strategies presented are the basics of the Defense in Depth policy. The IATF outlines the five classes of attack and how the layers of the Defense in Depth policy (people, operations, technology) provide protection against these different threats. Table 1 provides examples of how the layered defenses help mitigate the five classes of attacks.

Table 1. Layered Defense

| Class of Attack | First Line of Defense | Second Line of Defense |
|---|---|---|
| Passive | Network layer encryption | Security enabled application |
| Active | Defend the enclave | Defend the computing environment |
| Insider | Personnel Security | Access Controls |
| Close-In | Physical Security | Technical Surveillance |
| Distribution | Trusted Software development | Run time integrity controls |

Source: National Security Agency. Information Assurance Technical Framework 3.1. (Fort Meade, September 2002), 2-13.

The government also developed other approaches to improving information security and information assurance. One venture was the establishment of InfraGard. A joint venture between the government and industry, InfraGard exists to educate members on current information threats and protection measures (Federal Bureau of Investigation 2002). Local InfraGard members offered to assist with this research project in an effort to further exchange ideas and solutions related to providing information assurance.

Government employees involved in providing information assurance have also produced commercially available materials to assist IT personnel with managing security risks. One of the more recent selections is *Information Assurance*, written by two Department of Defense IT professionals, Joseph Boyce and Dan Jennings. *Information Assurance* explains the defense in depth concept in simple terms and also provides a checklist used by military units, government agencies, and corporations to determine the comprehensiveness of their information assurance plans and policies (Boyce and Jennings 2002, xii). Boyce and Jennings' work serves as the bridge from the government to the civilian view of information assurance.

## Civilians and Information Assurance

What do those outside of the military and government think of information assurance? While not adopting the phrase "information assurance" until recently, the civilian sector produced several articles and publications from 1998 until the present dealing with ensuring data integrity and network security. The literature from the private sector can be further distinguished based on the support received either from the civilian sector or the military-industrial sector.

The military-industrial sector uses their focused expertise to publish articles and periodicals that analyze current efforts and technologies that support Information Assurance within the Joint Community. SIGNAL magazine, published by the Armed Forces Communications and Electronics Association, provides a monthly review of Joint and service-specific technologies and efforts being used in the information assurance battle. The September 2002 edition of SIGNAL magazine provided an overview of efforts being made by the private sector in providing critical infrastructure security. The post September 11th world has seen an increase in outreach between government and industry (Ackerman 2002, 19).

Another military-industrial viewpoint can be found in the publications of the National Defense Research Institute (RAND). In August 2000, RAND produced an analysis of the Pacific Command's security efforts in their report *Advanced Network Defense Research.* Prepared for the National Security Agency, this analysis provides a case study review of Defense Department efforts to monitor and protect networks in the PACOM area of operations. More importantly, the review offers several new technologies and operations that are required to improve information security (National Defense Research Institute 2000, 2-6). RAND has also produced several other publications to include *Countering the New Terrorism.* This collection of essays helps define the existing and predicted threats against military technologies and American infrastructure.

However, the government is not the only sponsor of, or educator for, information assurance research. Individual corporations and corporate alliances have recently encouraged open discussion of information assurance and the role of network security in

protecting both the availability and reliability of data. One such alliance is the Human Firewall council. The Human Firewall council started in an attempt to educate corporations and users on the "human issues" involved in providing information assurance and network security. Essentially a grassroots organization, the Human Firewall council has the support of several leading organizations and companies in the information security arena. Several of these organizations, to include the Information Systems Security Association (ISSA) and BSI Global, combined to develop the Security Management Index. The Security Management Index is based on ISO 17799 and provides a framework for measuring the effectiveness of a corporation's information assurance plans and policies (Human Firewall 2002).

The Information Systems Security Association (ISSA) also maintains their own website that provides an outlet for security personnel to receive training, share ideas, and obtain certification. The ISSA sponsors local area workshops that deal with current challenges in providing information assurance and network security (ISSA 2002). The local ISSA chapter assisted this research project by providing access to various white papers and offering attendance at quarterly workshops.

The SANS (SysAdmin, Audit, Network, Security) Institute is another organization that focuses on educating, training, and certifying IT personnel in the areas of system administration and network security. Their website offers multiple case studies of defense in depth practices in addition to single layer network security solutions. One case study in particular, "Defense in Depth: A Small University Takes Up the Challenge," offers a unique perspective on establishing a multi-layered network defense with limited resources. In addition, the author references several other non-military and

government examples of a defense in depth approach to network security (Robinson 2002). Another case study, “Defense in Depth: A Primer,” offers the civilian reader an introduction the Defense in Depth policy outlined in IATF 3.1 and implemented by the Department of Defense (VanMeter 2001). Both of these case studies reflect a trend of corporate IT professionals examining the military’s and government’s approach to providing information assurance.

What general principles do civilians apply in order to provide information assurance? From the civilian sector, earlier writings focused on data integrity and network security. One recent publication, *A Practical Guide to Security Engineering and Information Assurance*, provided current case studies of information assurance in the workplace. The Internet sites of Computerworld and NewsFactor provide a weekly analysis of new products and technologies along with reporting on trends related to information assurance.

## Why is Information Assurance Important?

As early as 1996, former Director of Central Intelligence John Deutch warned that several countries were developing the techniques and tactics to conduct offensive information attacks against the United States. In the same year, the General Accounting Office released a study declaring “the Department of Defense’s computer systems are being attacked everyday.” While the total number of attempts to attack or hack the military’s information systems were unknown, Defense Department officials estimated that the number of attacks could have been as high as 250,000 (Larson and Peters 2001, 110-112). All of this while the military began moving more administrative information

and services online. The military's network for unclassified processing is the NIPRNET. And while the NIPRNET is the military's primary tool for electronic commerce, logistics, and other information system processes, the NIPRNET is not entirely separate from the internet. The NIPRNET connects to the internet through 17 gateways. The internet, and the commercially owned and maintained transmission lines, is still the primary path for the information traffic of the military. The bottom line interconnectivity of the internet effects the military as well (Kent 2003).

This interconnectivity comes with a price. The price is the military's vulnerability to damage of their information or information systems. As discussed in Chapter 1, the United States is most vulnerable to Information Warfare for three reasons. First, the United States is the most information dependent country in the world. The United States military, economy, and culture are all dependent on information. Lieutenant Colonel Kevin Kennedy, author of the *Grand Strategy for Information Age National Security,* described the United States as the "most wired" country. Second, as the most dependent country on information, the United States is also the most vulnerable country to information attacks. Third, the same technology the United States uses to share information can be used by adversaries to impact on the political and cultural fabric of the American society (Kennedy, Lawlor, and Nelson 1997, 2).

"Information warfare will be the most complex type of warfare in the 21st century, and it will decide who will win and who will lose the war." This statement was made not by an information warrior for the United States, but rather by Colonel Chang Mengxiong in the publication Chinese View of Future Warfare (Kent 2003). The view of the United States is similar. As early as 1999, then Deputy Secretary of Defense John Hamre

declared, “We’re in the middle of a cyber war” (Larson and Peters 2002, 112). The current director of the Defense Information Systems Agency stated, “information systems must be controlled, protected, and managed as effectively as weapon systems” (Kent 2003). Information assurance is the means to protect and defend information and information systems and ensure their availability to the warfighter at the critical time.

But are the military’s information systems vulnerable? Are the military’s information systems under attack? The comments of potential adversaries notwithstanding, a review of recent detected activity against the NIPRNET shows a dramatic increase in potential attempts to gain access to the unclassified systems of the military. Figure 1 outlines the recent activity detected by the Joint Task Force – Computer Network Operations against the NIPRNET from 1994 to 2002.

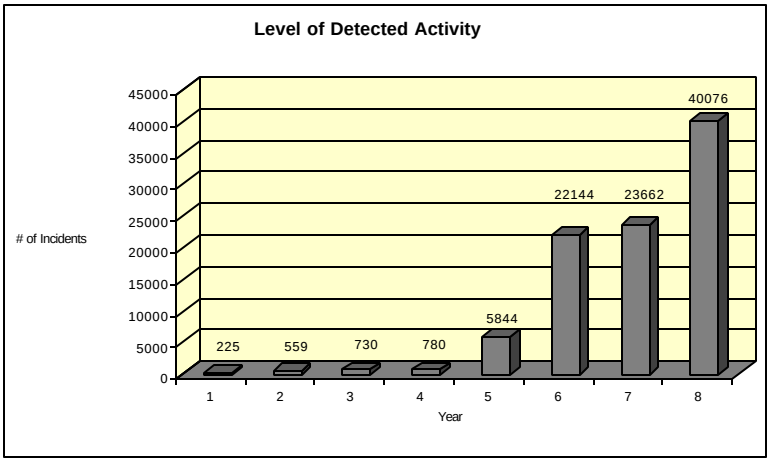



Fig. 1. Level of Detected Activity Against the NIPRNET *Source:* Presentation by MAJ Gary Kent given at the US Army Command and General Staff College, 04 Feb 03.

Beyond the statistics, a walk through any major bookstore revels several viewpoints of the strategies and tactics involved in information warfare and the need for information assurance. The sub-title to James Adams' *The Next World War* makes the bold proclamation "computers are the weapons and the front line is everywhere." Adams approaches the future of warfare as being conducted with and about information and information systems (Adams 1998, 13). Adams' views are similar to those held by John Arquilla and David Ronfeldt in their book *In Athena's Camp.* Arquilla and Ronfeldt espouse the future of netwar and cyberwar. While these new descriptions of conflict are met with some resistance, and even hostility, the basic components of the described future conflicts are information and information systems (Arquilla and Ronfeldt 1997, 27-32). The conflicts described in these books and others, such as *Secrets & Lies, Digital Security in a Networked World*, provide the worst-case scenarios for information assurance in the future.

Other publications provide insight into the mind of the adversary while giving examples of current tactics and techniques being used to attack computers and networks. The popular *Hacking Exposed* series provides the information security professional with an overview of network security threats and solutions. Describing the world today as "a chaotic battlefield", authors Stuart McClure, Joel Scambray, and George Kurtz offer the network administrator a look inside the mind of the hacker. By introducing the proliferation of hacker activity, the authors stress the importance of information security plans, policies, and training (McClure, Scambray and Kurtz 2001, xxv).

## Conclusion

The president of the Armed Forces Communications and Electronic Association (AFCEA), Vice Admiral Herbert A. Browne recently compared information in today's world with the presence of oxygen in the air. Both of them are essential and in some cases omnipresent. In his commentary, Vice Admiral Browne continued:

> (Information) is an essential part of life, . . . And its denial or contamination can be life-altering or even fatal . . . Information sharing must be recognized as an international resource . . . Just as the oxygen we breathe must be unadulterated and undenied, so must information remain pure . . . The only solution to our information security challenges is to demand full information assurance . . . (and) both industry and government must recognize that this is the requirement. (Browne 2002, 14)

Vice Admiral Browne's commentary outlines the three basic facts that all military and civilian leaders and IT personnel must recognize today. First, information is vital to the daily operations of the military and the corporate world. Second, information assurance includes the actions taken to protect information and the information systems. Finally, the military and industry must both develop plans that provide for information assurance in today's interconnected world. One way for the military IT professionals to evaluate if the Defense in Depth policy is providing "full information assurance" is to compare their performance with their civilian counterparts.

# CHAPTER 3

# RESEARCH METHODOLOGY

This research thesis will be based on a literature review of Information Assurance combined with a comparative analysis of standardized interviews of personnel involved in providing information services outside of the military. The literature review established baseline answers to several of the secondary research questions:

What is Information Assurance?

Why is Information Assurance important to the military?

How does the Defense in Depth approach provide for Information Assurance? The literature review also offered some insight into how corporate America provides Information Assurance. The focus of this study, however, and the primary question is does the Defense in Depth policy offer the Army an advantage over the corporate world in providing information assurance.

## Survey Participants

In order to answer the primary question, this researcher surveyed four information security professionals. The first participant was an Information Assurance Manager working at the Directorate of Information Management (DOIM) at a mid-sized Army installation. As the Information Assurance Manager, he is responsible for the network and information security of the entire installation to include subordinate commands and organizations. The interview with the Information Assurance Manager provided a standardized sample of Army compliance with the Defense in Depth approach and what the Army considers “effective” protection. The Information Assurance Manager’s

firsthand knowledge of current techniques, tactics, and procedures will serve as the balance to his civilian counterparts.

The second interviewee was an Information Systems Administrator for a national level government agency. This Administrator has over thirty years in the information security business. He offered unique insights into both the roles and actions of a government agency in providing information assurance. He also provided the perspective of another government organization outside the military that falls under the general guidelines outlined in the National Security Agency's Information Assurance Technical Framework. The participation of the government agency demonstrated the effectiveness of civilian administrators in developing strategies to provide information assurance for their organizations.

The third participant was a web developer and information systems manager for a small privately owned web development firm. On the economic frontlines, the web developer provides web design and web maintenance services for several Fortune 500 companies. His interaction with managers of IT departments and marketing personnel places him in a unique position to comment on the current efforts being made to secure business networks and provide data integrity.

The final participant was a network security manager at a state level university. Working at one the "training camps" for the current and next generation of network users, the university security manager provides network services for over 30,000 students, educators, and support personnel across several facilities on, and off, the centralized campus. His interaction with researchers and students that stretch the limits of network security gives him unique insights into the challenges of information assurance.

## Survey Structure

Steiner Kvale described two metaphors of interviewers in his work *InterViews.* The first interviewer is a miner. As a miner, the interviewer digs data out of the subject to be compared with an objective standard. The second interviewer is a traveler. As a traveler, the interviewer roams freely through a conversation with the subject in an attempt to find new knowledge (Kvale 1996, 3-5). For the purpose of this study, the researcher attempted to be both miner and traveler.

Each interview was structured around a series of questions developed by the Human Firewall Council. With approval of the Director of the Human Firewall Council, this study used the questions contained in the Security Management Index to interview each participant. The individual sections of the SMI are similar to the ten domains of information security as defined by the International Information Systems Security Certifications Consortium (ISC2). While the ISC2 developed the ten domains as part of the common body of knowledge for information security professionals, the Human Firewall council developed the ten sections of the SMI to correlate with the actual information operations of the average survey participant. The ninety-nine questions contained in the ten sections are based on the ISO 17799 standard for information security. Table 2 lists the ten sections of the Security Management Index survey and how they compare to the ten domains of information security (Miller and Gregory 2002, 17-22).

Table 2. Comparison of SMI and ISC2 Security Domains

| Security Management Index Sections | 10 Domains of Information Security |
|---|---|
| Information Security Policy | Security Management Practices |
| Security Organization | Security Architecture |
| Asset Classification and Control | Cryptography |
| Personnel Security | Operations Security |
| Physical and Environmental Security | Physical Security |
| Communications and Operations Management | Telecommunications & Network Security |
| Access Control | Access Control Systems & Methodology |
| Systems Development and Maintenance | Applications & Systems Development Security |
| Business Continuity Management | Business Continuity Planning |
| Compliance | Law, Investigations, & Ethics |

*Source*: Security Management Index, Human Firewall Project, www.humanfirewall.org

For the purpose of the SMI, each survey participant answered the questions according to one of the five responses contained in Table 3. These basic responses, mined by the researcher (Kvale 1996, 4), were entered into the Human Firewall Council's web based survey to obtain a SMI score.

The SMI scoring methodology is designed to provide additional weighting for standards considered minimum across the industry, such as the use of virus protection on network systems. The weights applied to each question are listed in Appendix A. An organization must, however, be implementing all standards to obtain a score of 100 percent. Each organization's score is based on their percentage obtained of the maximum available for that section. As an example, the information security policy section contains six standards, or questions. The maximum score for this section, including weighting, would be 180 points. An organization that was fully compliant in five standards and

partially compliant in the sixth would score 165 points or 92 percent (Human Firewall 2002).

Table 3. Security Management Index Responses

| Response | Definition | Value in Security Management Index |
|---|---|---|
| Fully Compliant | Objective fully implemented | 10 |
| Partially Compliant | Objective has been partially implemented | 5 |
| Planned | Organization has definite plans to implement objective | 2 |
| Not Compliant or Planned | The organization has not implemented the standard and does not a plan to implement | 0 |
| Not Applicable | The objective does not apply to the organization | No score given Potential score not included |

*Source*: Security Management Index, Human Firewall Project, www.humanfirewall.org

## Survey Limitations and Bias

For this study, the Security Management Index offers a method of obtaining quantitative data for over 1,000 survey participants. At the conclusion of the interviews, the answers obtained by the study are added to the SMI database. The results provided by the Human Firewall Council include not only a score for the four participants but also the average score for all participants. While a detailed quantitative analysis is beyond the scope of this study, the use of the overall index for comparison will help determine the performance of the Defense in Depth policy in providing information assurance for the military.

This study gained a unique perspective from conducting the interviews personally rather than asking the participants themselves to enter the data into the SMI database. First, use of pre-existing questions helped in creating an unbiased survey. Though the researcher is a military professional, initial bias was in favor of civilian solutions to the information assurance challenge. The pre-existing questions, developed by civilian IT professionals and based on an independent standard (ISO 17799), reduced the effects of the researcher's initial opinions. Second, through the interview process, this study gained additional insights into why the participants feel they are not compliant with certain standards or why a standard does not apply to their organization. When the interview ventured away from the standard responses, the researcher assumed the role of traveler (Kvale 1996, 5). In this part of the research, the conversation offered the knowledge. The standardized interviews with IT personnel outside the military offered a unique perspective on the efforts being made outside the gated community. As a result of the interaction during the interview process, a qualitative analysis on the participants' responses will help determine if the Defense in Depth approach offers any advantage.

The time constraints of the MMAS program limit the possible number of interviews. However, the diversity of the current SMI population will allow for results to be applicable despite the small number of interviews. This data should help compare military networks with a large variety of civilian IT organizations. The qualitative analysis of information gained from the literature review, the standardized interviews, and quantitative analysis of the Security Management Index responses will help identify and highlight any differences between the military's approach and corporate America's approach to information assurance. This triangulation of data is the basis for the

comparative analysis. The frame of reference is information assurance. The Security Management Index provides the grounds of comparison (Walk 1998). The assumption for comparison is that a higher score on the SMI would indicate the organization does a better job in providing information assurance. At the end of the study, the research should be able to determine if the Defense in Depth approach provides military IT professionals with an advantage over their civilian counterparts for providing Information Assurance for the NIPRNET or if incorporating practices used in the corporate world would improve the Defense in Depth approach.

# CHAPTER 4

## ANALYSIS

Using the Security Management Index as a ruler, how does the Army measure up to other organizations in providing information assurance? Based on an interview with the Information Assurance Manager (IAM) at an Army installation's Directorate of Information Management (DOIM), this study obtained answers to questions posed by the Human Firewall Council in their Security Management Index survey. The study submitted these answers to Human Firewall in order to obtain a Security Management Index score for the DOIM. Complete results for the DOIM can be found in Appendix B. In order to provide a means of comparison, this researcher also interviewed information security personnel in three other organizations: a government agency, a web development company, and a university. Complete results for the government agency, the web developer, and the university can be found in appendices C, D, and E, respectively. Using the same questions developed by the Human Firewall Council, the study submitted the answers for each organization and obtained a separate Security Management Index score for each organization. The Human Firewall Council also provided the average scores for their entire survey, over 1000 participants. Figure 2 depicts the overall Security Management Index (SMI) score for each organization in the study along with the overall average SMI score computed by the Human Firewall Council.

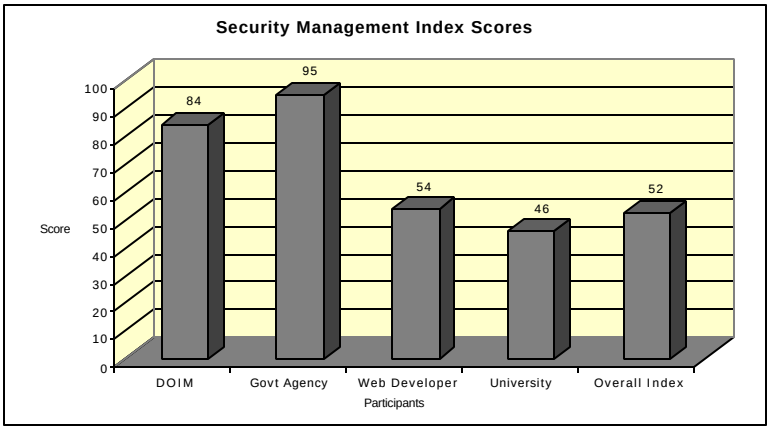



Fig. 2. Security Management Index Results

The overall SMI for the DOIM is 84 percent compared to a national index of 52 percent. An initial review of baseline scores would indicate the Defense in Depth policy offers the Amy network administrator a significant advantage in providing for information assurance. However, the overall score only tells part of the story. In order to determine what specific advantages, if any, the Defense in Depth policy provides, an examination of the individual sections that comprise the SMI must be undertaken.

Each interview was structured around a series of questions developed by the Human Firewall Council. With approval of the Director of the Human Firewall Council, this study used the questions contained in the Security Management Index to interview each participant. The Human Firewall Council designed the questions based on the ISO 17799 standard for information security. The 99 questions are spread across the ten sections listed in Table 4.

Table 4

| Security Management Index Sections |
| --- |
| Information Security Policy |
| Security Organization |
| Asset Classification and Control |
| Personnel Security |
| Physical and Environmental Security |
| Communications and Operations Management |
| Access Control |
| Systems Development and Maintenance |
| Business Continuity Management |
| Compliance |

*Source*: Security Management Index, Human Firewall Project, www.humanfirewall.org

## Security Policy

The DOIM scored 100 percent on the security policy section. The structure and regulatory guidance that exist for the Army and other government agencies helps enforce and monitor compliance with approved practices and policies. One area to consider at the DOIM level is a review by legal and human resource representatives of the information security policies. The Information Assurance Manager at the DOIM felt this review was not applicable for the Army at the installation level since higher commands are providing direction and oversight. The assumption made by the Information Assurance Manager is that the higher commands have conducted a legal review of security policies applicable for the installation. Though not required by regulatory guidance or policy at the installation level, a review by human resources and legal representatives of the security policy might identify areas that could be improved with additional clarification or training. Figure 3 depicts the security policy scores for the participants.

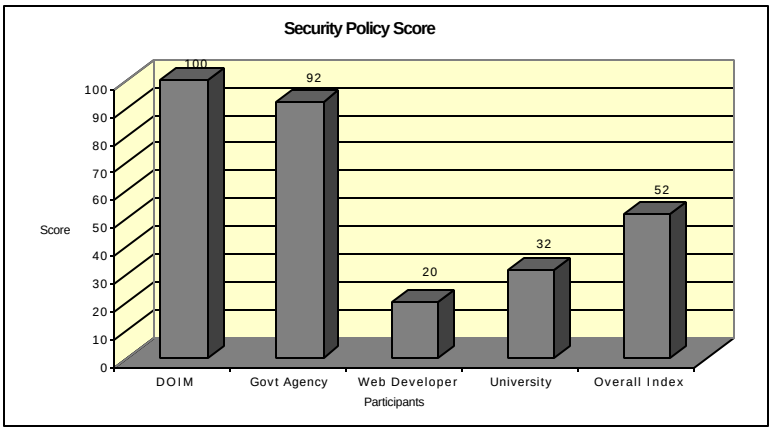



Fig. 3. Security Policy Scores

## Organizational Security

DOIM scored 89 percent in the area of organizational security. Compared to an overall average of 43 percent, the DOIM appears to be enjoying an advantage as a result of the Defense in Depth policy. The largest distracter for the DOIM is the consolidation of all information assurance roles under one individual. While the Army likes to stress unity of command, ownership, and responsibility, the burden of providing information assurance is quite demanding for one individual at an installation of the size supported by the DOIM.

At the interviewed DOIM, the Information Assurance Manager (IAM) carries the responsibilities of both physical security and automation security in addition to serving as a network manager. This multi-tasking does not allow the IAM the opportunity to focus on the overall picture. The government agency actually delegates the automation security role to one individual and the communication security role to a second individual. A third

individual serves as the Information Security Manager while also supervising the physical security team. Working as a team, they are able to provide a holistic approach to information assurance. Their performance and policies led them to a score of 100 percent for organizational security.

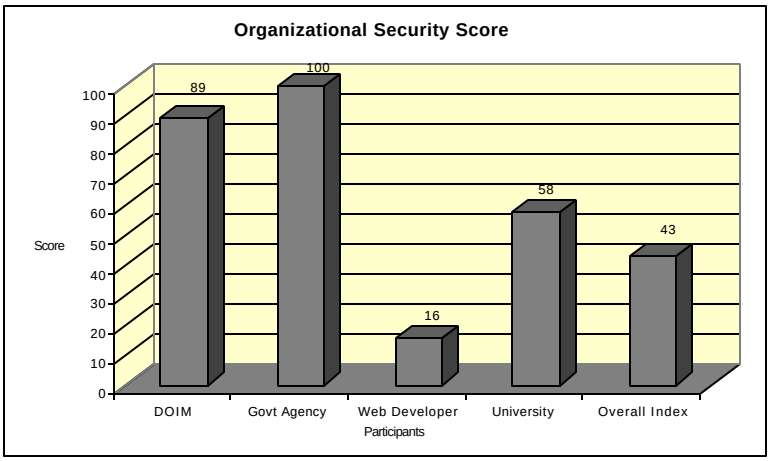



Fig. 4. Organizational Security Scores

## Asset Classification and Control

DOIM also scored 100 percent in the area of asset classification and control. Figure 5 portrays the results for the study group.

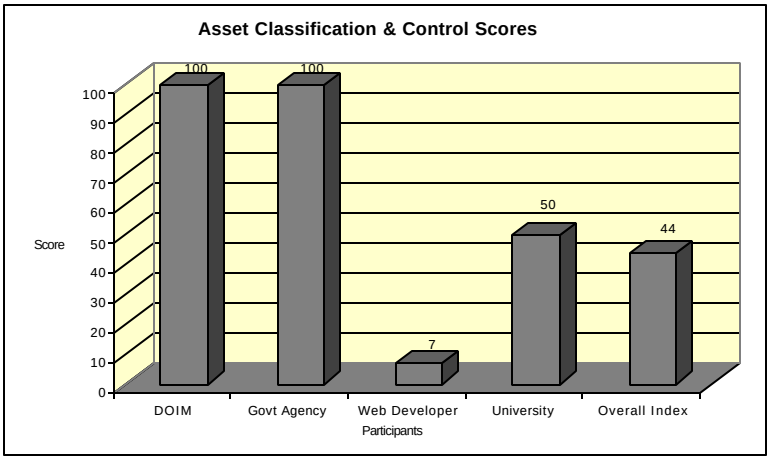



Fig. 5. Asset Classification and Control Scores

Once again, the regulatory guidance and the Defense in Depth policy help support the DOIM's performance in this area. For the people layer of Defense in Depth, the DOIM provides education and training for users in regards to the military classification system. The military classification system itself is the part of the operations level of the Defense in Depth policy. Here again, the DOIM benefits from an established procedure in the military of data classification as Unclassified, For Official Use Only, Secret, Top Secret, or Top Secret/SCI. Finally, the technological layer of the Defense in Depth policy allows the DOIM to use separate machines, or systems, for processing data of different classifications.

The government agency in the study also uses the same classification system and scored 100 percent in the area of asset classification and control. In comparison with the other organizations, the DOIM has a clear advantage. But why the struggle with asset classification for the web development company and the SMI participants? According to the web development company, data is all of one classification, propriety for the company. However, the legandary hacker Kevin Mitnick reviewed this common flaw in his book *The Art of Deception.* According to Mitnick, if information in the company is not classified then all the information is vulnerable to an outside exploiter. Conversely, if all the information in the company is close hold or highly classified then the company is not operating at peak efficiency. The balance lies in an asset classification policy based on the sensitivity of the data to the company's operations. In addition, the asset classification policy must establish guidelines for controlling who has access to the different classifications of data (Mitnick 2002, 272). The area of asset classification and control is one area in which civilian organizations can learn from the Army and the Defense in Depth policy. While companies might not be able to afford the dollar expense of separate systems for different levels of classified data, they can establish a simple issue-specific policy in regards to data classification. At the people layer, employees can be trained on the different classifications of assets, or data, and when and how the data is to be shared internally, or externally.

## Personnel Security

In the area of personnel security, the DOIM begins to find some significant challenges. Though the personnel security score of 60 percent is considered passing, the

DOIM could implement some of the steps from the civilian organizations to improve in this area of providing information assurance.

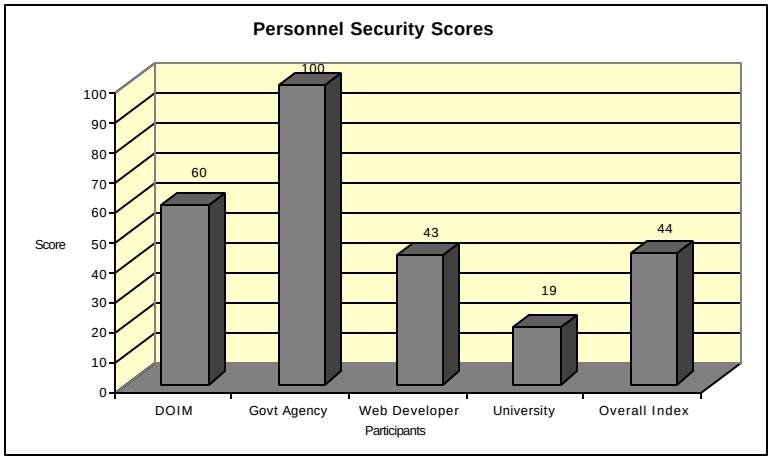



Fig. 6. Personnel Security Scores

One of the challenges with the DOIM in this study is the transient nature of the majority of their users. As with most military organizations, the DOIM experiences a significant turnover of personnel annually. The Information Assurance Manager stressed that all personnel are screened but not every user signs a non-disclosure agreement or has security roles and responsibilities outlined in their job descriptions. For the web developer, the confidentiality agreement is non-negotiable. For the majority of the civilian organizations, the confidentiality is the one program policy that clearly outlines for the user the purpose of security and the dangers of non-compliance. Joseph Boyce and Dan Jennings in their book *Information Assurance* outlined the value of employee training and education. Boyce and Jennings focused on the absolute requirement to

educate, train, and make employees aware of their role in providing information assurance for the organization. The theory is that as employees are trained and educated, the number of security incidents will decline. And employee training is more than the non-disclosure agreement. Boyce and Jennings recommended a program with four components: introductory training, briefings, information assurance handbook, and ongoing awareness training (Boyce and Jennings 2002, 175-179). For the DOIM, such a program would have to be part of the overall Army policy on information assurance training. The currently required briefs on Subversion, Espionage, and Operational Security could include the ongoing information assurance training recommend by Boyce and Jennings. In addition, the DOIM could establish a system-specific policy for their more transient users. This policy would outline the legal responsibilities for security of the users and also serve as non-disclosure agreement. Of course, such a policy would benefit from the previously mentioned review by legal and human resource representatives.

## Physical and Environmental Security

Located inside a fenced military installation with limited access and military police inspecting visitors at the gate, the DOIM is on track to score well in the areas of physical and environmental security. The DOIM scored 96 percent in the area of physical and environmental security, well above the overall average of 63 percent.

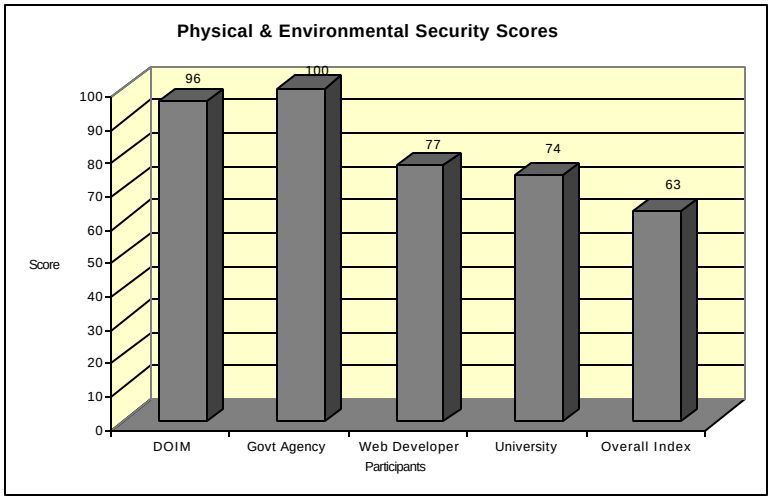



Fig. 7. Physical and Environmental Security Scores

The interview with the Information Assurance Manager for the DOIM did identify two areas of policy that might benefit from procedures at the other organizations. The first is in the area of general controls and relates to a clear desk and clear screen policy. At a regional security seminar presented by the Federal Bureau of Investigation and the Kansas City Chapter of the American Society for Industrial Security (ASIS), Bryan Hurd presented several scenarios in which an insider, or one posing as an insider, could create an information assurance problem by obtaining data off a messy desk or an unobserved computer screen. Mr. Hurd is a former counter-intelligence officer for the United States Navy and currently serves as an information security consultant in the Washington, DC area. In one account, Mr. Hurd related the dangers of removable media left unattended. Another account provided information on new technologies used for capturing images off a computer screen (Hurd 2002). The government agency in the study has a strict program policy in place regarding clear desks and clear screens. As a

result they scored 100 percent in this area. The Information Assurance Manager for the DOIM does have a unique challenge in that a large percentage of the workstations at the installation are shared. And in one way this helps with providing information assurance. Each user must log on prior to beginning work and should log off prior to departure. The training listed above combined with reminders about desk clutter would continue to improve the DOIM's performance in this area.

The second area in which the DOIM could improve is in the area of site selection and layout. The Information Assurance Manager for the DOIM is restricted on the amount and locations of the facilities available for network operations. However, there is clear value added to multiple server locations. The web development company in the study displaces their servers in two separate states to ensure availability. Current changes in the Army's network management approach, to include the new Network Operations Command, could offer the DOIM an alternative or further restrict the individual installations in location of key processing facilities.

## Communications and Operations Management

The Communications and Operations Management section deals with both operational responsibilities and security procedures for informational exchange. The DOIM scored well above the SMI standard score with 93 percent. However, the survey results would suggest that improvements could be made in two areas of operations management and in one area of communications policy.

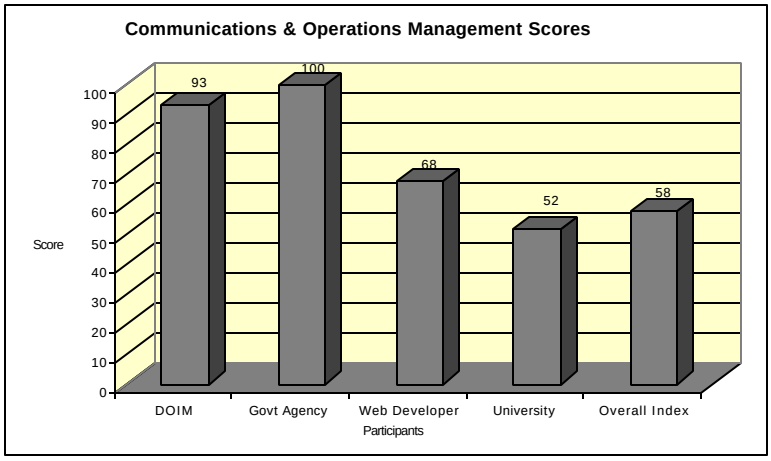



Fig. 8. Communications and Operations Management

In the area of operations management, the Information Assurance Manager for the DOIM replied that their capacity planning procedures were only partially implemented. Capacity planning is designing the network to handle the maximum number of expected users (Microsoft 2003). In *A Practical Guide to Security Engineering and Information Assurance*, Debra Herrmann stressed the dangers in the lack of capacity planning. Herrmann outlined how the lack of capacity planning creates vulnerabilities in the Open Systems Interconnection (OSI) seven-layer model. Specifically, failure to adequately anticipate network demands and compare them to planned network capacity creates vulnerabilities at the data link, network, and transport layers (Herrmann 2002, 150). For the DOIM, capacity planning is challenging based on the changes in operational tempo for Army units. With the increase in Army deployments or missions in new areas of operations, the DOIM experiences an increase in demand from internal and external

users. Both the government agency and the web development company base their capacity planning on absolute peak demand models.

The second challenge for the DOIM reference operations management is storage of system documentation. The Information Assurance Manager has policies in place for the installation. The challenge is in monitoring and enforcing compliance with the subordinate organizations under the DOIM's service umbrella.

The final challenge for the DOIM in the area of communications and operations management deals with security policies for electronic office systems. The Information Assurance Manager felt that while policies were in place for system usage and electronic mail, the DOIM did not have full implementation across the installation for establishing policy on or monitoring voice mail, mobile telephone usage, and postal services. The DOIM does perform well in coordinating the subordinate organizations that provide and utilize video teleconference services. This challenge is one of size. The web development company with 7 employees and limited external information exchange via video or postal services can more easily establish and enforce policies. The DOIM has over 6,500 users with multiple telephone lines across the installation. The government agency benefits from a second representative assigned the role of communications security.

## Access Control

Information assurance ensures availability, integrity, confidentiality, authentication, and non-repudiation. According to Bruce Schneier in his book *Secrets and Lies,* access control is the key to providing information assurance. In the simplest of terms, Schneier stated, "we want to make sure that authorized people are able to do

whatever they are authorized to do, and that everyone else is not" (Schneier 2000, 122). In what might be the most critical area for an organization to perform well in while providing information assurance, the DOIM scored 80 percent. Compared to the overall Human Firewall SMI average of 56 percent, the DOIM is well on the way to training personnel, implementing policies, and employing technologies to provide the highest levels of information assurance. However, improvements can almost always be made. In this critical area, the government agency recorded their lowest score of the study, and the web development company recorded one of their highest scores. Complete results for the access control section are shown in figure 9.

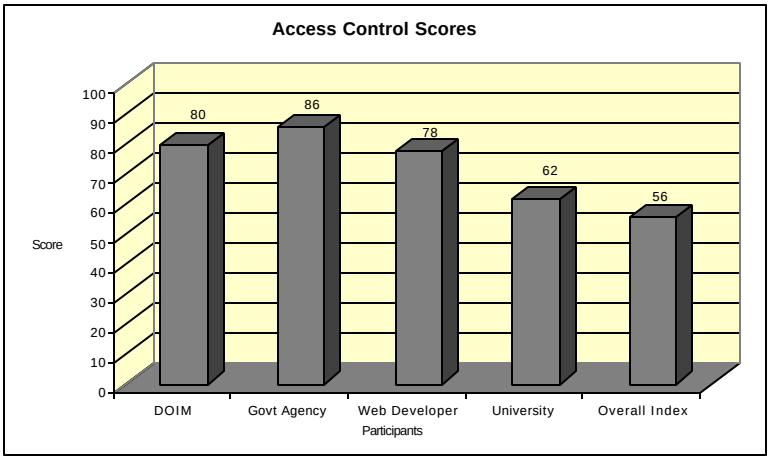



Fig. 9. Access Control Scores

As discussed in the review of physical and environmental security, the DOIM has the advantage of discouraging physical access by residing inside the gated military installation. However, access control is really about access to information. According to

Boyce and Jennings in *Information Assurance*, there are two basic methods of applying access controls: default permit and default deny. Default permit is the method of denying access only by exception while allowing open access for everyone else. Default deny is the opposite; allowing access only by exception and denying access for everyone else (Boyce, and Jennings 2002, 17). The government agency works on a default deny policy. As a result, the government agency accepts some risks in not automatically logging out users when equipment is unattended. The government agency also accepts some risks with regards to internal network connections. Within their network, the government agency does not except any external requests since their policies and architecture do not support external connections. The DOIM also works off a default deny policy.

The Information Assurance Manager stressed that the environment of shared computers and near continuous operations that experience un-forecasted user surges creates challenges with several of the SMI standards. The DOIM does not log out users when equipment is left unattended. Users often login to complete initial work at the beginning of the duty day and then spend the rest of the workday away from their terminal. The DOIM does not feel the cost-benefit gain is high enough to implement automatic log-off across the installation. However, certain subordinate units on the installation include automatic log-off for some of the web-based applications.

In comparison, the web development company ensures that unattended equipment is logged off automatically. The web development company examines the idea from a unique perspective. According to the president of the company, leaving the connections to the network open just allows more traffic to pass through the network that can be observed and exploited. The effort to login does not result in a dramatic loss of

productivity. Loss of sensitive data, or non-sensitive data that can be leveraged to gain sensitive data, is a dramatic loss of productivity (Web Development Interview 2003).

The second challenge for the DOIM deals with password selection and use. All three organizations in the study control password allocation through a formal management process. According to the Human Firewall Council, only 33 percent of the organizations participating in the SMI survey reported controlling password allocation through a formal management process (Human Firewall 2002). The difference is in the organizations' requirements to follow good security practices in the selection and use of passwords. Both the government agency and the web development company maintain formal control of the password selection process. Some of the subordinate organizations at the DOIM are required to change passwords after six months, but the DOIM does not formally control the selection. In *The Art of Deception,* Kevin Mitnick discussed password management and control in detail. Mitnick offered nine separate policies for an organization regarding passwords. The policy on selecting passwords recommended four separate requirements for selecting passwords: password length of eight to twelve characters; password contents to include upper and lower case, numbers, and special characters; password contents to not include any word in a dictionary; and new passwords should not be a variant of a previous password (Mitnick 2002, 319-320). When requiring users to change their passwords, the DOIM could develop a simple script that would compare the users new password choice against the above or similar criteria. Though the process would take additional time, the benefit of reducing vulnerabilities and increasing information assurance would be worth the small inconvenience.

Systems Development and Maintenance

According to Boyce and Jennings in *Information Assurance*, system development is "the process for designing, developing, installing, and testing new systems to ensure their compliance with established security requirements" (Boyce and Jennings 2002, 218). The eighth part of the Security Management Index focuses on system development and maintenance. The Human Firewall designed the SMI for use by various organizations to include software development. While this part of the SMI is more of a focus for the web development company, some of the questions and areas discussed are considerations for the DOIM. Figure 10 reflects the scores for the organizations for system development and maintenance.

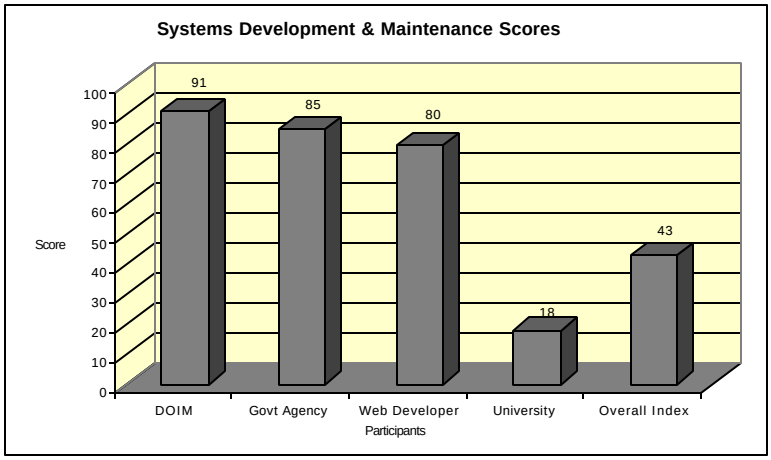



Fig. 10. Systems and Development and Maintenance Scores

As mentioned in Chapter 2, system development includes the design, construction, implementation, operation, and maintenance of the information systems

(Applegate, McFarlan, and McKenney 1999, 31). The survey questions regarding the security process of system files and development processes (construction, implementation, and maintenance phases) are not applicable to the DOIM. However, the questions regarding security requirements and cryptographic controls (design and operation phases) are of primary concern for the DOIM and the installation it supports. The DOIM score of 91 percent in the areas of system development and maintenance indicates they are on track for providing a high level of information assurance. The challenge lies in the application of digital signatures.

Digital signatures and digital certificates are designed to assist with the authentication and non-repudiation portions of information assurance (Herrmann 2002, 173). A digital signature can help answer the questions of "who are we communicating with?" and "did you really send the message you claimed to have sent?". The challenge for the Information Assurance Manager is full implementation of digital signature acceptance across the installation. Since the passage of the Electronic Security Act in 2000, electronic signatures have official status (Herrmann 2002, 173). However, in a military culture that still values paper over electrons, digital signatures are not a bridge too far but merely a bridge not yet crossed.

## Business Continuity Management

Business continuity management is perhaps the one area that presents the DOIM with the largest challenges. DOIM scored 20 percent in the area of business continuity management. However, business continuity management is also the lowest performance area for the web development company and the university. Yet, the government agency

again scored 100 percent. And for the Human Firewall survey, the average score for all 1,072 participants is only 41 percent, the lowest average score across the ten categories.

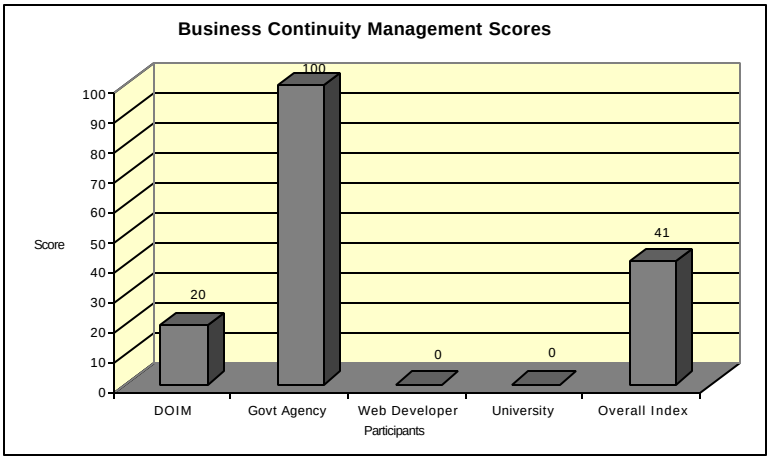



Fig. 11. Business Continuity Management Scores

Ironically enough, this is probably the one area where the oversight and structure appear to hinder the Information Assurance Manager in the attempt to provide the highest levels of information assurance. The DOIM has a requirement to develop a business continuity plan, or contingency plan. However, since a large majority of the supervision and oversight are currently focused on daily operations, long term planning suffers. But a focus on availability is the core of business continuity. Business continuity planning is the solution to the question "will this network always be available?". Boyce and Jennings in *Information Assurance* focused on four areas of contingency planning: backups, uninterruptible power supply, disaster recovery, and continuity of operations. The information technology managers must develop and implement plans that determine what

information should be backed up and how often. Daily operations depend on the availability of power, either through regular service, battery backup, or generator systems. Disaster recovery procedures address the organization's response to natural or man-made disasters. The continuity of operations plans provide the documented steps to continuing operations during or immediately after a disaster, either at the primary location or at an identified alternate site (Boyce and Jennings 2002, 171-172).

After the September 11 terrorist attacks, financial service companies and other organizations experienced the effects of untested contingency planning. The Bank of New York had a state-of-the-art network architecture, redundant data paths into and out of each Manhattan office, and several backup systems. Yet, according to Donald Monks, Bank of New York senior vice president, they still experienced total communications failure. The point of failure was actually in the central office of the telecommunications company that provided the redundant data paths. Now Bank of New York and other industry leaders are requiring telecommunications carriers to guarantee not only diversified network routes but also redundancy throughout the infrastructure (Junnarkar 2002).

Scoring a 100 percent on the Human Firewall survey, the government agency has met the standard for continuity planning. The government agency has established a well documented and rehearsed continuity plan. The government agency can continue operations at a remote site with very little loss of operational capability. The DOIM is developing their plans for continuity operations. For the Information Assurance Manager, the challenge is not in conducting the risk analysis, nor in determining the critical systems required for normal operations. The challenge is in developing a plan that meets

the approval of the higher headquarters that would need to provide the appropriate resources, systems, and locations to support full operational capability at a remote site.

## Compliance

The final category of the Human Firewall survey is compliance: compliance with legal, technical, and security requirements. The DOIM scored 79 percent in the area of compliance. The biggest challenge for the DOIM and the government agency regarding compliance dealt with internal and external review of security and technical standards. The DOIM does not have complete implementation across the installation with subordinate departments adhering to the policy requiring routine self-assessments. Neither the government agency nor the DOIM have fully implemented external review. The Information Assurance Manager does receive assistance inspections and compliance inspections from higher headquarters but does not receive assistance from outside the Department of Defense. The government agency also does not request or receive any external review outside of their organization.

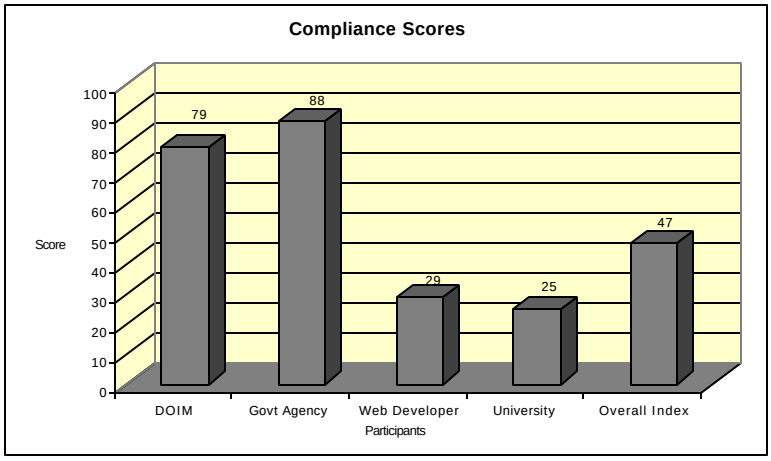



Fig. 12. Compliance

## Conclusion

How does the Army measure up against the corporate competition? In regards to the standards developed by the Human Firewall Council for the Security Management Index, the representative for the Army, the DOIM, scored well above the overall SMI average of 54 percent. For the purpose of this study, the DOIM significantly out-performed the web development company and the university but was out-scored by the government agency. Does the Defense in Depth policy offer the Army network administrator an advantage? Yes, but several factors work in the Army's favor to create this advantage. And the corporate sector does offer some accepted practices that could further increase the Army's ability to provide information assurance. The two primary SMI sub-sections in which standardized corporate practices would benefit the Army are in organizational security and personnel security.

In the area of organizational security, command focus and shared responsibilities would improve the ability of the local DOIM to provide full information assurance. While the DOIM scored well above the SMI average, additional focus in these areas would further enhance the DOIM's ability to provide information assurance. First, the use of an installation-wide steering committee with command support would help create the guiding coalition that could continually monitor information assurance efforts and reinforce the need for compliance. Second, while the Army likes to stress unity of command, ownership, and responsibility, the burden of providing information assurance is quite demanding for one individual at an installation of the size supported by the DOIM. Allocation of the responsibilities for physical security and network manager to other personnel would allow the Information Assurance Manager the opportunity to focus on the overall picture of full information assurance.

For personnel security, the Army could benefit from the use of non-disclosure agreements. For the majority of the civilian organizations, the confidentiality is the one program policy that clearly outlines for the user the purpose of security and the dangers of non-compliance. Though some military organizations use confidentiality statements for classified programs, the use of similar statements for all network users is not common, at least not within at the DOIM surveyed in this study. An annual program requiring the signature of a non-disclosure agreement would reinforce network users' information handling responsibilities.

# CHAPTER 5

# CONCLUSION AND RECOMMENDATIONS

Does the Defense in Depth policy offer an advantage to the Army network administrators in providing for information assurance? Yes in that the Defense in Depth policy allows an organization to score better on the Security Management Index developed by the Human Firewall Council. The assumption is that the Security Management Index (SMI) score reflects on how well an organization provides information assurance; a higher SMI score would indicate a higher level of information assurance. Future research would be able to take the study to the next step. An analysis of successful root level attacks versus total number of attacks identified would provide an indication of integrity. A report on network and application usage would provide an indication of availability. Standards of measure for ensuring authentication, confidentiality, and non-repudiation would be harder to establish.

## Infosec Warriors

Does the Defense in Depth policy offer an advantage to the Army network administrators in providing for information assurance? Yes, but the Army and the military in general has a larger hierarchy and budget for security concerns and information assurance. As infosec warriors, the military has a requirement to provide availability, integrity, authentication, and confidentiality. On the administrative side, failure to provide information assurance for the NIPRNET can result in loss of sensitive but unclassified data. However, on the tactical side, failure to provide an adequate level of information assurance can result in the death of a soldier.

For the Objective Force, information assurance becomes even more critical to mission readiness and accomplishment. The information assurance key performance parameter for the Objective Force network requires 95 percent protection against all external and known threats by 2008. For the fielding of the Objective Force in 2032, the information assurance measures must be able to protect against 99 percent of all external and known threats (Roeber 2003).

The ability of the Army network administrator to provide information assurance is a transient skill. Every day the information warfare threat increases. From sophisticated foreign capabilities to the teenage hacker, military networks face a daily electronic assault. The proliferation of viruses and "script kiddies" can mask the more deliberate asymmetric threat of special interest groups or nation states. The military network administrator has to provide protection both at the home-station and at forward deployed locations without the benefit of the local DOIM. At a recent conference on information security, Brigadier General Gregory J. Premo, Deputy Chief of Staff for Information Management at the U.S. Army Training and Doctrine Command, spoke on the need for commanders to understand that the old mentality of "Sparky fix that" will not solve the problem. Information assurance is not an information technology "thing." Information assurance is commander's business (Premo 2003). And information assurance is becoming very important commander's business. During the course of this study, the daily brief provided to the Army Chief of Staff changed. The briefings provided today include a status of the posted Information Assurance Vulnerability Alerts (IAVA). Distributed by the Army Computer Emergency Response Team (ACERT), the IAVAs notify military and civilian IT professionals of current vulnerabilities to information

systems as a result of viruses, malicious code, or other security flaws. Now in addition to current deployment status and other operational issues, the senior uniformed Army officer is briefed on the information assurance status of all major installations.

## Infosec Cowboys

The commercial sector has a limited responsibility and requirement to provide information assurance. It lacks the structured hierarchy and the regulatory requirements. For civilians providing information assurance is subject to the same cost analysis as building a new factory or opening a new storefront -- what is the cost of providing information assurance versus the benefit gained? What is the risk to the common corporation? Loss of credit cards? Defaced web sites? Loss of proprietary information? Attacks on networks in the corporate world (if basic security measures have been applied) almost always carry a sympathetic response from the populace. The president of the web development company said it best when examining the information assurance steps taken in the corporate world, “we are at best infosec cowboys and at worst negligent” (Web development interview).

If imitation is the highest form of flattery, then the Defense in Depth policy does offer an advantage. During the course of the study and the interaction with the Human Firewall Council, new technologies and services appeared on the market in order to help organizations with providing information security and information assurance. Todd Tucker of NetIQ, one of the primary authors of the Security Management Index report, discussed the development of their product as being modeled on the Defense in Depth policy outlined in the Information Assurance Technical Framework produced by the

National Security Agency (Tucker interview). A review of the NetIQ website highlights the newest products and services available to assist with information management and security. An exploration of the newest solution, VigilEnt, uncovers the three components of this integrated security management: people, operations, and technology (www.NetIQ.com).

## The Road Ahead

In February of 2003, President Bush released the National Strategy to Secure Cyberspace. In the opening pages, the President stated:

> The cornerstone of America's cyberspace security strategy is and will remain a public-private partnership. The federal government invites the creation of, and participation in, public-private partnerships to implement this strategy. Only by acting together can we build a more secure future in cyberspace. (National Strategy, iii)

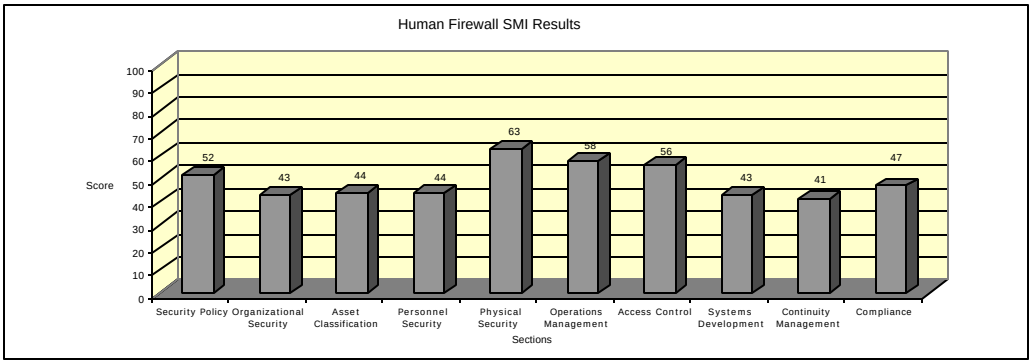
The guidance from the President is clear. Even though the federal government has the responsibilities and resources to better provide information assurance, the participation of private organizations in sharing methods and technologies that work is critical to providing the best level of information assurance. At a recent technology conference, Mister Richard Hale, Chief Executive Officer for Information Assurance for DISA, explained that the genesis for the development of the Defense in Depth DMZ plan was a result of reviewing best e-business practices (Hale 2003). Identification, and application, of industry technologies and operations that support better security will further enhance the military's ability to provide information assurance.

The Defense in Depth policy currently offers the best framework for providing information assurance. However, the threats and technologies continue to change. As the

military develops new equipment, tactics, and organizations to fight threats in the physical world, they must also change in the cyber world. The military must continue to train users in new tactics of defense and smart computer practices. The military must develop new technologies that prevent both insider and outsider attacks. And the military must modify existing operations to take advantage of policies and procedures that provide "full information assurance." To expand on the motto of the Human Firewall council, if the military is aware and responsible, then they can be secure.

APPENDIX A

BASIC SURVEY QUESTIONS




*Source*: Security Management Index, Human Firewall Project, www.humanfirewall.org

## I. SECURITY POLICY

| Weighting | | Fully Implemente | Partially Implemente | Planned | Not Implemente d or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **The current information security policies within your organization:** | | | | | | |
| 3 | Define information security objectives and illustrate the importance of security. | | | | | | |
| 3 | Provide a statement of management's intentions to support information security. | | | | | | |
| 3 | Define general responsibilities for employees | | | | | | |
| 3 | Reference other corporate documents. | | | | | | |
| | **When reviewing, evaluating, and distributing security policies, your organization:** | | | | | | |
| 3 | Specifies a distinct information security owner who has the responsibility for update and maintenance of those policies. | | | | | | |
| 3 | Requires a review by business owners, legal and HR. | | | | | | |

## II. ORGANIZATIONAL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization's information security infrastructure is supported by an:** | | | | | | |
| 2 | Enterprise-wide security steering committee. | | | | | | |
| 2 | Information security representative from each business unit. | | | | | | |
| 3 | Allocation of information security responsibilities. | | | | | | |
| 2 | Information security advisor (for expert advice) or coordinator (to coordinate security knowledge sharing). | | | | | | |
| 2 | Documented points of contact with law enforcement, standards setting organizations, and service providers for both incident response support and security advice. | | | | | | |
| 2 | Autonomous oversight of information security policy implementation. | | | | | | |
| 2 | Performing risk assessments before granting access to external parties. | | | | | | |
| 2 | Management review and approval for the development or implementation of any new information technologies. | | | | | | |
| | **Third party access is controlled in your organization by:** | | | | | | |
| 3 | Documenting the organization's security policy in the third-party contracts. | | | | | | |
| 1 | Educating third-parties on the information classification program. | | | | | | |

**II. ORGANIZATIONAL SECURITY (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Outsourcing is controlled in your organization by:** | | | | | | |
| 3 | Communicating legal requirements for protecting your organization's information and information technologies and services. | | | | | | |
| 1 | Educating outsourcers on their liabilities in regards to the security of your organization's information, technologies and services. | | | | | | |

## III. ASSET CLASSIFICATION & CONTROL

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization accounts for key information technology assets by:** | | | | | | |
| 1 | Recording the information and business ownership. | | | | | | |
| | **Safeguarding information within your organization includes:** | | | | | | |
| 3 | A simple, effective guideline that indicates the degree of protection for each type of information asset. | | | | | | |
| 3 | Handling and labeling procedures for physical media. | | | | | | |

## IV. PERSONNEL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has policies and procedures in place that require:** | | | | | | |
| 2 | Information security roles and responsibilities included in all company job descriptions. | | | | | | |
| 3 | All candidates for employment be adequately screened to ensure that their qualifications are accurate. | | | | | | |
| 3 | All employees sign a confidentiality (non-disclosure) agreement to ensure that they understand their information handling responsibilities. | | | | | | |
| | **An organizational-wide training program is in place for:** | | | | | | |
| 3 | Information security policy and procedure awareness and comprehension. | | | | | | |
| 2 | Informing personnel of their legal responsibilities for security. | | | | | | |
| 2 | Correct usage of information technologies including business applications. | | | | | | |
| | **In response to a security incident or malfunction, a formal process exists in your organization that:** | | | | | | |
| 2 | Instructs employees on the correct method of handling security incidents. | | | | | | |
| 1 | Instructs employees on the proper method for preserving the evidence necessary for forensic investigations. | | | | | | |
| 3 | Disciplines employees who have violated security policies and procedures. | | | | | | |

## V. PHYSICAL & ENVIRONMENTAL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Facilities are properly secured by:** | | | | | | |
| 3 | Adequately establishing and monitoring a physical perimeter. | | | | | | |
| 3 | Logging and supervising physical entry by visitors. | | | | | | |
| 2 | Taking precautions (including proper layout and site selection) to secure against natural or man-made disasters. | | | | | | |
| 2 | Adequately controlling personnel or third parties working in secure areas. | | | | | | |
| 2 | Controlling delivery and loading areas and if possible, isolating them from information processing facilities. | | | | | | |
| 3 | Protecting equipment from power failures and other electrical anomalies. | | | | | | |
| | **Equipment is properly secured by:** | | | | | | |
| 2 | Protecting power and telecommunications cabling from interception or damage. | | | | | | |
| 3 | Correctly maintaining equipment to ensure its continued availability and integrity. | | | | | | |
| 3 | Physically destroying storage devices containing sensitive information or securely overwriting sensitive data when disposing of those storage devices. | | | | | | |

## V. PHYSICAL & ENVIRONMENTAL SECURITY (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization prevents the compromise or theft of information and information-processing facilities by requiring:** | | | | | | |
| 1 | A clear desk policy for papers and removable storage media, and a clear screen policy for information processing facilities. | | | | | | |
| 2 | Equipment or information taken off site to be removed only with authorization, and proper logging is in place to control removal. | | | | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization ensures the correct and secure operation of information technologies by using:** | | | | | | |
| 3 | Documented standard operating procedures including processing information, scheduling, error handling, support, and recovery. | | | | | | |
| 3 | A change management process. | | | | | | |
| 2 | An incident management process. | | | | | | |
| 3 | An enforceable segregation of duties policy. | | | | | | |
| 3 | A separation between the development and operational (production) facilities. | | | | | | |
| | **Your organization minimizes the risk that essential systems will fail by using acceptable:** | | | | | | |
| 3 | Capacity planning. | | | | | | |
| | **Your organization protects the integrity and security of essential software and information by:** | | | | | | |
| 3 | Using a policy requiring compliance with software licenses. | | | | | | |
| 2 | Using a policy for obtaining files and software from third parties. | | | | | | |
| 3 | Installing and regularly updating anti-virus detection and repair software. | | | | | | |
| 3 | Checking any files, electronic mail attachments or downloads of uncertain origin for viruses before use. | | | | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization maintains the integrity and availability of essential information processing and communication services by:** | | | | | | |
| 3 | Implementing a backup and recovery process. | | | | | | |
| 3 | Logging operator commands. | | | | | | |
| 3 | Logging network and system faults. | | | | | | |
| | **Your organization ensures the protection of networks and supporting infrastructure by:** | | | | | | |
| 3 | Establishing special controls to safeguard the confidentiality and integrity of data passing over public networks. | | | | | | |
| 2 | Separating operational responsibility for the networks from the computer operations where possible. | | | | | | |
| | **To prevent asset damage and business activity interruption, your organization's media should be controlled and physically protected by:** | | | | | | |
| 3 | Procedures for managing removable computer media such as CDs, disks, and printed reports. | | | | | | |
| 3 | Securely storing system documentation. | | | | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization prevents loss, modification, or misuse of information exchanges between organizations by utilizing the appropriate:** | | | | | | |
| 2 | Agreements between organizations for the exchange of information. | | | | | | |
| 2 | Security precautions for electronic commerce. | | | | | | |
| 2 | Security precautions for electronic mail. | | | | | | |
| 2 | Security precautions for electronic office systems such as voice mail, mobile communications, video, and postal services. | | | | | | |
| 3 | Security precautions for publicly available systems such as web servers. | | | | | | |

## VII. ACCESS CONTROL

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization controls access to sensitive information by:** | | | | | | |
| 1 | Documenting policy and business requirements for controlling access to each business application. | | | | | | |
| 2 | Establishing access control rules that grant permissions to each group of users. | | | | | | |
| | **Your organization prevents unauthorized access to information systems by:** | | | | | | |
| 2 | Using a formal user registration and de-registration procedure for granting access to all multi-user information systems. | | | | | | |
| 2 | Controlling password allocation through a formal management process. | | | | | | |
| | **To prevent unauthorized user access, your organization requires users to:** | | | | | | |
| 3 | Follow good security practices in the selection and use of passwords. | | | | | | |
| 3 | Ensure that unattended equipment automatically logs users out or securely locks the system from unauthorized use. | | | | | | |
| | **The protection of networked services is enforced by:** | | | | | | |
| 3 | Authenticating all users from external connections. | | | | | | |
| 3 | Requiring authentication for an automatic connection to a network, such as in trust relationships between computers. | | | | | | |

## VII. ACCESS CONTROL (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **All access to computer resources is restricted by operating system controls that:** | | | | | | |
| 1 | Authenticate connections using terminal identification when it is important to ensure logins occur only from specific locations and/or computers or terminals. | | | | | | |
| 3 | Require a unique, non-descript identifier for all authorized users. | | | | | | |
| 3 | Employ effective password management systems that ensure quality passwords. | | | | | | |
| 2 | Restrict and log all use of system utilities. | | | | | | |
| 2 | Permit time-of-day connection limits to high-risk or sensitive applications. | | | | | | |
| | **All access and use of computer systems is monitored to detect unauthorized activities by:** | | | | | | |
| 3 | Recording all relevant security events in audit logs. | | | | | | |
| 3 | Reviewing audit logs through an effective and routine process. | | | | | | |
| 2 | Documenting and implementing procedures for monitoring the use of information technologies. | | | | | | |
| 2 | Using a process to ensure that all system clocks are synchronized with an agreed standard. | | | | | | |

**VII. ACCESS CONTROL (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has information security policies and procedures documented and implemented to control:** | | | | | | |
| 2 | The use of all mobile computing facilities including physical protection, access controls, cryptographic techniques, backups, and virus protection. | | | | | | |
| 3 | All activities related to working remotely from a fixed site not located within your organization. | | | | | | |

## VIII. SYSTEMS DEVELOPMENT AND MAINTENANCE

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization specifies security requirements and specifications that:** | | | | | | |
| 2 | Reflect the business value of the information assets involved. | | | | | | |
| 2 | Follow a risk assessment and risk management process to determine the acceptable controls. | | | | | | |
| | **Your organization uses cryptographic systems and techniques to protect the confidentiality, authenticity, or integrity of information by:** | | | | | | |
| 2 | Considering regulatory restrictions that may apply to the use of cryptographic algorithms in different parts of the world. | | | | | | |
| 2 | Applying digital signatures to any form of legal or business document being processed electronically. | | | | | | |
| 3 | Implementing a system for the management of cryptographic keys. | | | | | | |
| | **System files are secured during IT projects and support activities by:** | | | | | | |
| 2 | Controlling program source libraries in the development process to restrict possible corruption or tampering. | | | | | | |

## VIII. SYSTEMS DEVELOPMENT AND MAINTENANCE (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **In order to minimize the corruption of information systems, your organization controls the implementation of changes by:** | | | | | | |
| 3 | Using access controls to restrict the movement of programs and data from development into production. | | | | | | |
| 2 | Testing the application system when a change in the operating system occurs to ensure that there is no adverse impact on operation or security. | | | | | | |
| 2 | Conducting source code reviews to eliminate possible security vulnerabilities. | | | | | | |

## IX. BUSINESS CONTINUITY MANAGEMENT

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has a business continuity planning process in place that:** | | | | | | |
| 3 | Has produced a current, comprehensive, documented, and routinely-maintained business continuity plan for the entire organization. | | | | | | |
| 2 | Requires the completion of a business impact analysis that identifies events and their associated risks. | | | | | | |
| 2 | Requires a current prioritization of all business processes and supporting functions, including computer systems and applications. | | | | | | |
| 2 | Ensures that the business continuity plan is routinely tested using effective techniques to assure that the plan is viable. | | | | | | |

## X. COMPLIANCE

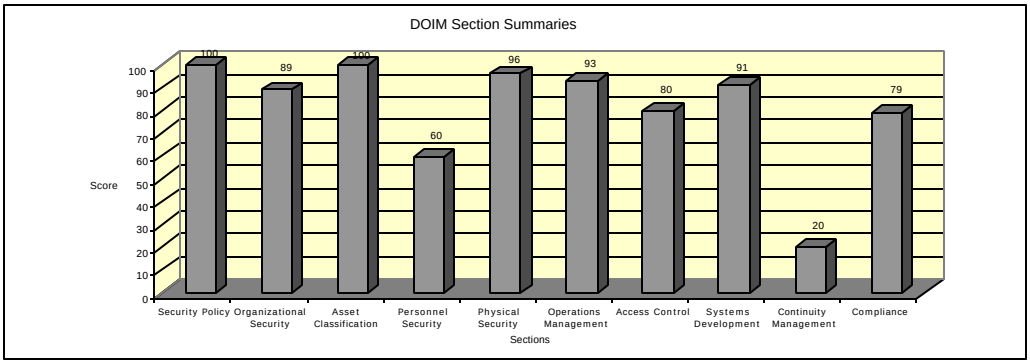
| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has implemented policies and procedures to ensure compliance with legal requirements that specifically address the:** | | | | | | |
| 3 | Data protection and privacy of personal information. | | | | | | |
| 3 | Acceptable use of information technologies. | | | | | | |
| 2 | International usage or transport of cryptographic controls. | | | | | | |
| | **Compliance procedures are in place that require the:** | | | | | | |
| 3 | Departmental managers to perform routine self-assessments to ensure that their areas comply with security policies and standards. | | | | | | |
| 2 | Technical checking of information systems by independent experts for compliance with security standards and leading practices. | | | | | | |
| | **Audit procedures are in place that require:** | | | | | | |
| 2 | Review of all operational systems to minimize the risk of business process disruptions. | | | | | | |
| 2 | Restricted access to system audit tools to prevent misuse or compromise. | | | | | | |

## XI. OPEN RESPONSE QUESTIONS

| | |
|---|---|
| 1 | How does your organization provide information security / assurance? |
| 2 | Based on your experience are your peers doing a good job of providing information assurance? |
| 3 | Are the government agencies you work with doing a good job of providing information assurance? |
| 4 | What are your recommendations for other organizations? |
| 5 | What are your goals or plans to improve your ability to provide information assurance? |

APPENDIX B

DOIM SURVEY RESULTS




*Source*: Security Management Index, Human Firewall Project, www.humanfirewall.org

## I. SECURITY POLICY

| Weighting | | Fully Implemente | Partially Implemente | Planned | Not Implemente d or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **The current information security policies within your organization:** | | | | | | |
| 3 | Define information security objectives and illustrate the importance of security. | X | | | | | |
| 3 | Provide a statement of management's intentions to support information security. | X | | | | | |
| 3 | Define general responsibilities for employees | X | | | | | |
| 3 | Reference other corporate documents. | X | | | | | |
| | **When reviewing, evaluating, and distributing security policies, your organization:** | | | | | | |
| 3 | Specifies a distinct information security owner who has the responsibility for update and maintenance of those policies. | X | | | | | |
| 3 | Requires a review by business owners, legal and HR. | | | | | X | |

## II. ORGANIZATIONAL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization's information security infrastructure is supported by an:** | | | | | | |
| 2 | Enterprise-wide security steering committee. | | | | | X | |
| 2 | Information security representative from each business unit. | X | | | | | |
| 3 | Allocation of information security responsibilities. | | X | | | | |
| 2 | Information security advisor (for expert advice) or coordinator (to coordinate security knowledge sharing). | X | | | | | |
| 2 | Documented points of contact with law enforcement, standards setting organizations, and service providers for both incident response support and security advice. | X | | | | | |
| 2 | Autonomous oversight of information security policy implementation. | X | | | | | |
| 2 | Performing risk assessments before granting access to external parties. | X | | | | | |
| 2 | Management review and approval for the development or implementation of any new information technologies. | | X | | | | |
| | **Third party access is controlled in your organization by:** | | | | | | |
| 3 | Documenting the organization's security policy in the third-party contracts. | X | | | | | |
| 1 | Educating third-parties on the information classification program. | X | | | | | |

**II. ORGANIZATIONAL SECURITY (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Outsourcing is controlled in your organization by:** | | | | | | |
| 3 | Communicating legal requirements for protecting your organization's information and information technologies and services. | X | | | | | |
| 1 | Educating outsourcers on their liabilities in regards to the security of your organization's information, technologies and services. | X | | | | | |

## III. ASSET CLASSIFICATION & CONTROL

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization accounts for key information technology assets by:** | | | | | | |
| 1 | Recording the information and business ownership. | X | | | | | |
| | **Safeguarding information within your organization includes:** | | | | | | |
| 3 | A simple, effective guideline that indicates the degree of protection for each type of information asset. | X | | | | | |
| 3 | Handling and labeling procedures for physical media. | X | | | | | |

## IV. PERSONNEL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has policies and procedures in place that require:** | | | | | | |
| 2 | Information security roles and responsibilities included in all company job descriptions. | | | | X | | |
| 3 | All candidates for employment be adequately screened to ensure that their qualifications are accurate. | X | | | | | |
| 3 | All employees sign a confidentiality (non-disclosure) agreement to ensure that they understand their information handling responsibilities. | | X | | | | |
| | **An organizational-wide training program is in place for:** | | | | | | |
| 3 | Information security policy and procedure awareness and comprehension. | | X | | | | |
| 2 | Informing personnel of their legal responsibilities for security. | | X | | | | |
| 2 | Correct usage of information technologies including business applications. | | X | | | | |
| | **In response to a security incident or malfunction, a formal process exists in your organization that:** | | | | | | |
| 2 | Instructs employees on the correct method of handling security incidents. | X | | | | | |
| 1 | Instructs employees on the proper method for preserving the evidence necessary for forensic investigations. | X | | | | | |
| 3 | Disciplines employees who have violated security policies and procedures. | | X | | | | |

## V. PHYSICAL & ENVIRONMENTAL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Facilities are properly secured by:** | | | | | | |
| 3 | Adequately establishing and monitoring a physical perimeter. | X | | | | | |
| 3 | Logging and supervising physical entry by visitors. | X | | | | | |
| 2 | Taking precautions (including proper layout and site selection) to secure against natural or man-made disasters. | | | | | X | |
| 2 | Adequately controlling personnel or third parties working in secure areas. | X | | | | | |
| 2 | Controlling delivery and loading areas and if possible, isolating them from information processing facilities. | X | | | | | |
| 3 | Protecting equipment from power failures and other electrical anomalies. | X | | | | | |
| | **Equipment is properly secured by:** | | | | | | |
| 2 | Protecting power and telecommunications cabling from interception or damage. | X | | | | | |
| 3 | Correctly maintaining equipment to ensure its continued availability and integrity. | X | | | | | |
| 3 | Physically destroying storage devices containing sensitive information or securely overwriting sensitive data when disposing of those storage devices. | X | | | | | |

## V. PHYSICAL & ENVIRONMENTAL SECURITY (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization prevents the compromise or theft of information and information-processing facilities by requiring:** | | | | | | |
| 1 | A clear desk policy for papers and removable storage media, and a clear screen policy for information processing facilities. | | | | X | | |
| 2 | Equipment or information taken off site to be removed only with authorization, and proper logging is in place to control removal. | X | | | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization ensures the correct and secure operation of information technologies by using:** | | | | | | |
| 3 | Documented standard operating procedures including processing information, scheduling, error handling, support, and recovery. | X | | | | | |
| 3 | A change management process. | X | | | | | |
| 2 | An incident management process. | X | | | | | |
| 3 | An enforceable segregation of duties policy. | X | | | | | |
| 3 | A separation between the development and operational (production) facilities. | | | | | X | |
| | **Your organization minimizes the risk that essential systems will fail by using acceptable:** | | | | | | |
| 3 | Capacity planning. | | X | | | | |
| | **Your organization protects the integrity and security of essential software and information by:** | | | | | | |
| 3 | Using a policy requiring compliance with software licenses. | X | | | | | |
| 2 | Using a policy for obtaining files and software from third parties. | X | | | | | |
| 3 | Installing and regularly updating anti-virus detection and repair software. | X | | | | | |
| 3 | Checking any files, electronic mail attachments or downloads of uncertain origin for viruses before use. | X | | | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization maintains the integrity and availability of essential information processing and communication services by:** | | | | | | |
| 3 | Implementing a backup and recovery process. | X | | | | | |
| 3 | Logging operator commands. | X | | | | | |
| 3 | Logging network and system faults. | X | | | | | |
| | **Your organization ensures the protection of networks and supporting infrastructure by:** | | | | | | |
| 3 | Establishing special controls to safeguard the confidentiality and integrity of data passing over public networks. | X | | | | | |
| 2 | Separating operational responsibility for the networks from the computer operations where possible. | X | | | | | |
| | **To prevent asset damage and business activity interruption, your organization's media should be controlled and physically protected by:** | | | | | | |
| 3 | Procedures for managing removable computer media such as CDs, disks, and printed reports. | X | | | | | |
| 3 | Securely storing system documentation. | | X | | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization prevents loss, modification, or misuse of information exchanges between organizations by utilizing the appropriate:** | | | | | | |
| 2 | Agreements between organizations for the exchange of information. | X | | | | | |
| 2 | Security precautions for electronic commerce. | X | | | | | |
| 2 | Security precautions for electronic mail. | X | | | | | |
| 2 | Security precautions for electronic office systems such as voice mail, mobile communications, video, and postal services. | | X | | | | |
| 3 | Security precautions for publicly available systems such as web servers. | X | | | | | |

## VII. ACCESS CONTROL

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization controls access to sensitive information by:** | | | | | | |
| 1 | Documenting policy and business requirements for controlling access to each business application. | X | | | | | |
| 2 | Establishing access control rules that grant permissions to each group of users. | X | | | | | |
| | **Your organization prevents unauthorized access to information systems by:** | | | | | | |
| 2 | Using a formal user registration and de-registration procedure for granting access to all multi-user information systems. | X | | | | | |
| 2 | Controlling password allocation through a formal management process. | X | | | | | |
| | **To prevent unauthorized user access, your organization requires users to:** | | | | | | |
| 3 | Follow good security practices in the selection and use of passwords. | | X | | | | |
| 3 | Ensure that unattended equipment automatically logs users out or securely locks the system from unauthorized use. | | X | | | | |
| | **The protection of networked services is enforced by:** | | | | | | |
| 3 | Authenticating all users from external connections. | X | | | | | |
| 3 | Requiring authentication for an automatic connection to a network, such as in trust relationships between computers. | X | | | | | |

**VII. ACCESS CONTROL (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **All access to computer resources is restricted by operating system controls that:** | | | | | | |
| 1 | Authenticate connections using terminal identification when it is important to ensure logins occur only from specific locations and/or computers or terminals. | | | | X | | |
| 3 | Require a unique, non-descript identifier for all authorized users. | X | | | | | |
| 3 | Employ effective password management systems that ensure quality passwords. | | X | | | | |
| 2 | Restrict and log all use of system utilities. | X | | | | | |
| 2 | Permit time-of-day connection limits to high-risk or sensitive applications. | | | | | X | |
| | **All access and use of computer systems is monitored to detect unauthorized activities by:** | | | | | | |
| 3 | Recording all relevant security events in audit logs. | X | | | | | |
| 3 | Reviewing audit logs through an effective and routine process. | X | | | | | |
| 2 | Documenting and implementing procedures for monitoring the use of information technologies. | | | | X | | |
| 2 | Using a process to ensure that all system clocks are synchronized with an agreed standard. | X | | | | | |

**VII. ACCESS CONTROL (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has information security policies and procedures documented and implemented to control:** | | | | | | |
| 2 | The use of all mobile computing facilities including physical protection, access controls, cryptographic techniques, backups, and virus protection. | | | | | X | |
| 3 | All activities related to working remotely from a fixed site not located within your organization. | | | | | X | |

## VIII. SYSTEMS DEVELOPMENT AND MAINTENANCE

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization specifies security requirements and specifications that:** | | | | | | |
| 2 | Reflect the business value of the information assets involved. | X | | | | | |
| 2 | Follow a risk assessment and risk management process to determine the acceptable controls. | X | | | | | |
| | **Your organization uses cryptographic systems and techniques to protect the confidentiality, authenticity, or integrity of information by:** | | | | | | |
| 2 | Considering regulatory restrictions that may apply to the use of cryptographic algorithms in different parts of the world. | X | | | | | |
| 2 | Applying digital signatures to any form of legal or business document being processed electronically. | | X | | | | |
| 3 | Implementing a system for the management of cryptographic keys. | X | | | | | |
| | **System files are secured during IT projects and support activities by:** | | | | | | |
| 2 | Controlling program source libraries in the development process to restrict possible corruption or tampering. | | | | | X | |

**VIII. SYSTEMS DEVELOPMENT AND MAINTENANCE (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **In order to minimize the corruption of information systems, your organization controls the implementation of changes by:** | | | | | | |
| 3 | Using access controls to restrict the movement of programs and data from development into production. | | | | | X | |
| 2 | Testing the application system when a change in the operating system occurs to ensure that there is no adverse impact on operation or security. | | | | | X | |
| 2 | Conducting source code reviews to eliminate possible security vulnerabilities. | | | | | X | |

## IX. BUSINESS CONTINUITY MANAGEMENT

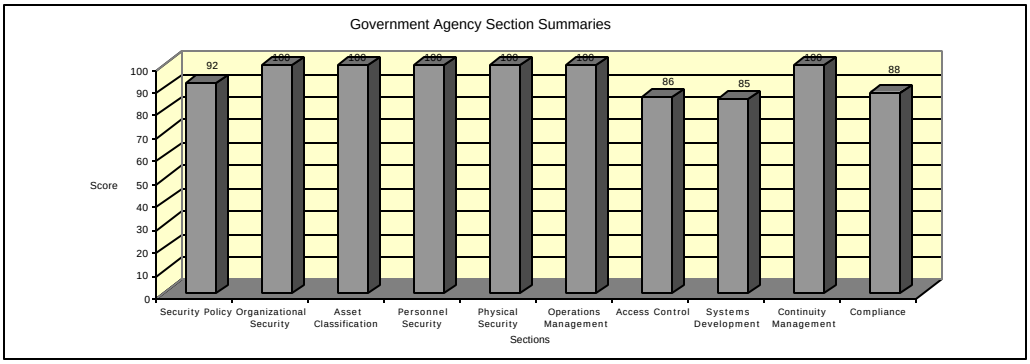
| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has a business continuity planning process in place that:** | | | | | | |
| 3 | Has produced a current, comprehensive, documented, and routinely-maintained business continuity plan for the entire organization. | | | X | | | |
| 2 | Requires the completion of a business impact analysis that identifies events and their associated risks. | | | X | | | |
| 2 | Requires a current prioritization of all business processes and supporting functions, including computer systems and applications. | | | X | | | |
| 2 | Ensures that the business continuity plan is routinely tested using effective techniques to assure that the plan is viable. | | | X | | | |

## X. COMPLIANCE

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has implemented policies and procedures to ensure compliance with legal requirements that specifically address the:** | | | | | | |
| 3 | Data protection and privacy of personal information. | X | | | | | |
| 3 | Acceptable use of information technologies. | X | | | | | |
| 2 | International usage or transport of cryptographic controls. | X | | | | | |
| | **Compliance procedures are in place that require the:** | | | | | | |
| 3 | Departmental managers to perform routine self-assessments to ensure that their areas comply with security policies and standards. | | X | | | | |
| 2 | Technical checking of information systems by independent experts for compliance with security standards and leading practices. | | X | | | | |
| | **Audit procedures are in place that require:** | | | | | | |
| 2 | Review of all operational systems to minimize the risk of business process disruptions. | | X | | | | |
| 2 | Restricted access to system audit tools to prevent misuse or compromise. | X | | | | | |

APPENDIX C

GOVERNMENT AGENCY RESULTS




*Source*: Security Management Index, Human Firewall Project, www.humanfirewall.org

## I. SECURITY POLICY

| Weighting | | Fully Implemente | Partially Implemente | Planned | Not Implemente d or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **The current information security policies within your organization:** | | | | | | |
| 3 | Define information security objectives and illustrate the importance of security. | X | | | | | |
| 3 | Provide a statement of management's intentions to support information security. | X | | | | | |
| 3 | Define general responsibilities for employees | X | | | | | |
| 3 | Reference other corporate documents. | | X | | | | |
| | **When reviewing, evaluating, and distributing security policies, your organization:** | | | | | | |
| 3 | Specifies a distinct information security owner who has the responsibility for update and maintenance of those policies. | X | | | | | |
| 3 | Requires a review by business owners, legal and HR. | X | | | | | |

## II. ORGANIZATIONAL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization's information security infrastructure is supported by an:** | | | | | | |
| 2 | Enterprise-wide security steering committee. | X | | | | | |
| 2 | Information security representative from each business unit. | X | | | | | |
| 3 | Allocation of information security responsibilities. | X | | | | | |
| 2 | Information security advisor (for expert advice) or coordinator (to coordinate security knowledge sharing). | X | | | | | |
| 2 | Documented points of contact with law enforcement, standards setting organizations, and service providers for both incident response support and security advice. | X | | | | | |
| 2 | Autonomous oversight of information security policy implementation. | X | | | | | |
| 2 | Performing risk assessments before granting access to external parties. | X | | | | | |
| 2 | Management review and approval for the development or implementation of any new information technologies. | X | | | | | |
| | **Third party access is controlled in your organization by:** | | | | | | |
| 3 | Documenting the organization's security policy in the third-party contracts. | X | | | | | |
| 1 | Educating third-parties on the information classification program. | X | | | | | |

**II. ORGANIZATIONAL SECURITY (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Outsourcing is controlled in your organization by:** | | | | | | |
| 3 | Communicating legal requirements for protecting your organization's information and information technologies and services. | X | | | | | |
| 1 | Educating outsourcers on their liabilities in regards to the security of your organization's information, technologies and services. | X | | | | | |

## III. ASSET CLASSIFICATION & CONTROL

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization accounts for key information technology assets by:** | | | | | | |
| 1 | Recording the information and business ownership. | X | | | | | |
| | **Safeguarding information within your organization includes:** | | | | | | |
| 3 | A simple, effective guideline that indicates the degree of protection for each type of information asset. | X | | | | | |
| 3 | Handling and labeling procedures for physical media. | X | | | | | |

## IV. PERSONNEL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has policies and procedures in place that require:** | | | | | | |
| 2 | Information security roles and responsibilities included in all company job descriptions. | X | | | | | |
| 3 | All candidates for employment be adequately screened to ensure that their qualifications are accurate. | X | | | | | |
| 3 | All employees sign a confidentiality (non-disclosure) agreement to ensure that they understand their information handling responsibilities. | X | | | | | |
| | **An organizational-wide training program is in place for:** | | | | | | |
| 3 | Information security policy and procedure awareness and comprehension. | X | | | | | |
| 2 | Informing personnel of their legal responsibilities for security. | X | | | | | |
| 2 | Correct usage of information technologies including business applications. | X | | | | | |
| | **In response to a security incident or malfunction, a formal process exists in your organization that:** | | | | | | |
| 2 | Instructs employees on the correct method of handling security incidents. | X | | | | | |
| 1 | Instructs employees on the proper method for preserving the evidence necessary for forensic investigations. | X | | | | | |
| 3 | Disciplines employees who have violated security policies and procedures. | X | | | | | |

## V. PHYSICAL & ENVIRONMENTAL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Facilities are properly secured by:** | | | | | | |
| 3 | Adequately establishing and monitoring a physical perimeter. | X | | | | | |
| 3 | Logging and supervising physical entry by visitors. | X | | | | | |
| 2 | Taking precautions (including proper layout and site selection) to secure against natural or man-made disasters. | X | | | | | |
| 2 | Adequately controlling personnel or third parties working in secure areas. | X | | | | | |
| 2 | Controlling delivery and loading areas and if possible, isolating them from information processing facilities. | X | | | | | |
| 3 | Protecting equipment from power failures and other electrical anomalies. | X | | | | | |
| | **Equipment is properly secured by:** | | | | | | |
| 2 | Protecting power and telecommunications cabling from interception or damage. | X | | | | | |
| 3 | Correctly maintaining equipment to ensure its continued availability and integrity. | X | | | | | |
| 3 | Physically destroying storage devices containing sensitive information or securely overwriting sensitive data when disposing of those storage devices. | X | | | | | |

**V. PHYSICAL & ENVIRONMENTAL SECURITY (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization prevents the compromise or theft of information and information-processing facilities by requiring:** | | | | | | |
| 1 | A clear desk policy for papers and removable storage media, and a clear screen policy for information processing facilities. | X | | | | | |
| 2 | Equipment or information taken off site to be removed only with authorization, and proper logging is in place to control removal. | X | | | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization ensures the correct and secure operation of information technologies by using:** | | | | | | |
| 3 | Documented standard operating procedures including processing information, scheduling, error handling, support, and recovery. | X | | | | | |
| 3 | A change management process. | X | | | | | |
| 2 | An incident management process. | X | | | | | |
| 3 | An enforceable segregation of duties policy. | X | | | | | |
| 3 | A separation between the development and operational (production) facilities. | | | | | X | |
| | **Your organization minimizes the risk that essential systems will fail by using acceptable:** | | | | | | |
| 3 | Capacity planning. | X | | | | | |
| | **Your organization protects the integrity and security of essential software and information by:** | | | | | | |
| 3 | Using a policy requiring compliance with software licenses. | X | | | | | |
| 2 | Using a policy for obtaining files and software from third parties. | X | | | | | |
| 3 | Installing and regularly updating anti-virus detection and repair software. | X | | | | | |
| 3 | Checking any files, electronic mail attachments or downloads of uncertain origin for viruses before use. | X | | | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization maintains the integrity and availability of essential information processing and communication services by:** | | | | | | |
| 3 | Implementing a backup and recovery process. | X | | | | | |
| 3 | Logging operator commands. | X | | | | | |
| 3 | Logging network and system faults. | X | | | | | |
| | **Your organization ensures the protection of networks and supporting infrastructure by:** | | | | | | |
| 3 | Establishing special controls to safeguard the confidentiality and integrity of data passing over public networks. | X | | | | | |
| 2 | Separating operational responsibility for the networks from the computer operations where possible. | X | | | | | |
| | **To prevent asset damage and business activity interruption, your organization's media should be controlled and physically protected by:** | | | | | | |
| 3 | Procedures for managing removable computer media such as CDs, disks, and printed reports. | X | | | | | |
| 3 | Securely storing system documentation. | X | | | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization prevents loss, modification, or misuse of information exchanges between organizations by utilizing the appropriate:** | | | | | | |
| 2 | Agreements between organizations for the exchange of information. | X | | | | | |
| 2 | Security precautions for electronic commerce. | | | | | X | |
| 2 | Security precautions for electronic mail. | X | | | | | |
| 2 | Security precautions for electronic office systems such as voice mail, mobile communications, video, and postal services. | X | | | | | |
| 3 | Security precautions for publicly available systems such as web servers. | | | | | X | |

## VII. ACCESS CONTROL

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization controls access to sensitive information by:** | | | | | | |
| 1 | Documenting policy and business requirements for controlling access to each business application. | X | | | | | |
| 2 | Establishing access control rules that grant permissions to each group of users. | X | | | | | |
| | **Your organization prevents unauthorized access to information systems by:** | | | | | | |
| 2 | Using a formal user registration and de-registration procedure for granting access to all multi-user information systems. | X | | | | | |
| 2 | Controlling password allocation through a formal management process. | X | | | | | |
| | **To prevent unauthorized user access, your organization requires users to:** | | | | | | |
| 3 | Follow good security practices in the selection and use of passwords. | X | | | | | |
| 3 | Ensure that unattended equipment automatically logs users out or securely locks the system from unauthorized use. | | X | | | | |
| | **The protection of networked services is enforced by:** | | | | | | |
| 3 | Authenticating all users from external connections. | | | | | X | |
| 3 | Requiring authentication for an automatic connection to a network, such as in trust relationships between computers. | | X | | | | |

**VII. ACCESS CONTROL (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **All access to computer resources is restricted by operating system controls that:** | | | | | | |
| 1 | Authenticate connections using terminal identification when it is important to ensure logins occur only from specific locations and/or computers or terminals. | X | | | | | |
| 3 | Require a unique, non-descript identifier for all authorized users. | X | | | | | |
| 3 | Employ effective password management systems that ensure quality passwords. | X | | | | | |
| 2 | Restrict and log all use of system utilities. | | X | | | | |
| 2 | Permit time-of-day connection limits to high-risk or sensitive applications. | | | | | X | |
| | **All access and use of computer systems is monitored to detect unauthorized activities by:** | | | | | | |
| 3 | Recording all relevant security events in audit logs. | X | | | | | |
| 3 | Reviewing audit logs through an effective and routine process. | | X | | | | |
| 2 | Documenting and implementing procedures for monitoring the use of information technologies. | X | | | | | |
| 2 | Using a process to ensure that all system clocks are synchronized with an agreed standard. | X | | | | | |

**VII. ACCESS CONTROL (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has information security policies and procedures documented and implemented to control:** | | | | | | |
| 2 | The use of all mobile computing facilities including physical protection, access controls, cryptographic techniques, backups, and virus protection. | X | | | | | |
| 3 | All activities related to working remotely from a fixed site not located within your organization. | X | | | | | |

## VIII. SYSTEMS DEVELOPMENT AND MAINTENANCE

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization specifies security requirements and specifications that:** | | | | | | |
| 2 | Reflect the business value of the information assets involved. | X | | | | | |
| 2 | Follow a risk assessment and risk management process to determine the acceptable controls. | X | | | | | |
| | **Your organization uses cryptographic systems and techniques to protect the confidentiality, authenticity, or integrity of information by:** | | | | | | |
| 2 | Considering regulatory restrictions that may apply to the use of cryptographic algorithms in different parts of the world. | X | | | | | |
| 2 | Applying digital signatures to any form of legal or business document being processed electronically. | | | | X | | |
| 3 | Implementing a system for the management of cryptographic keys. | X | | | | | |
| | **System files are secured during IT projects and support activities by:** | | | | | | |
| 2 | Controlling program source libraries in the development process to restrict possible corruption or tampering. | X | | | | | |

**VIII. SYSTEMS DEVELOPMENT AND MAINTENANCE (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **In order to minimize the corruption of information systems, your organization controls the implementation of changes by:** | | | | | | |
| 3 | Using access controls to restrict the movement of programs and data from development into production. | | | | | X | |
| 2 | Testing the application system when a change in the operating system occurs to ensure that there is no adverse impact on operation or security. | | | | | X | |
| 2 | Conducting source code reviews to eliminate possible security vulnerabilities. | | | | | X | |

## IX. BUSINESS CONTINUITY MANAGEMENT

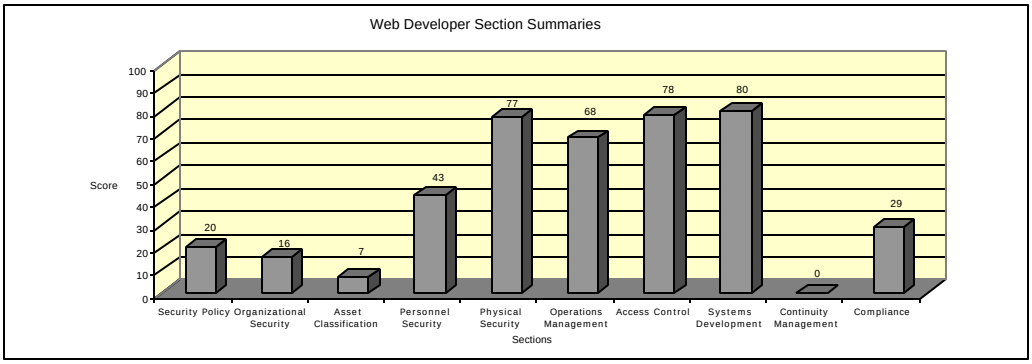
| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has a business continuity planning process in place that:** | | | | | | |
| 3 | Has produced a current, comprehensive, documented, and routinely-maintained business continuity plan for the entire organization. | X | | | | | |
| 2 | Requires the completion of a business impact analysis that identifies events and their associated risks. | X | | | | | |
| 2 | Requires a current prioritization of all business processes and supporting functions, including computer systems and applications. | X | | | | | |
| 2 | Ensures that the business continuity plan is routinely tested using effective techniques to assure that the plan is viable. | X | | | | | |

## X. COMPLIANCE

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has implemented policies and procedures to ensure compliance with legal requirements that specifically address the:** | | | | | | |
| 3 | Data protection and privacy of personal information. | X | | | | | |
| 3 | Acceptable use of information technologies. | X | | | | | |
| 2 | International usage or transport of cryptographic controls. | X | | | | | |
| | **Compliance procedures are in place that require the:** | | | | | | |
| 3 | Departmental managers to perform routine self-assessments to ensure that their areas comply with security policies and standards. | X | | | | | |
| 2 | Technical checking of information systems by independent experts for compliance with security standards and leading practices. | | | | X | | |
| | **Audit procedures are in place that require:** | | | | | | |
| 2 | Review of all operational systems to minimize the risk of business process disruptions. | X | | | | | |
| 2 | Restricted access to system audit tools to prevent misuse or compromise. | X | | | | | |

APPENDIX D

WEB DEVELOPER RESULTS




*Source*: Security Management Index, Human Firewall Project, www.humanfirewall.org

## I. SECURITY POLICY

| Weighting | | Fully Implemente | Partially Implemente | Planned | Not Implemente d or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **The current information security policies within your organization:** | | | | | | |
| 3 | Define information security objectives and illustrate the importance of security. | | X | | | | |
| 3 | Provide a statement of management's intentions to support information security. | | | | X | | |
| 3 | Define general responsibilities for employees | | X | | | | |
| 3 | Reference other corporate documents. | | | | | X | |
| | **When reviewing, evaluating, and distributing security policies, your organization:** | | | | | | |
| 3 | Specifies a distinct information security owner who has the responsibility for update and maintenance of those policies. | | | | X | | |
| 3 | Requires a review by business owners, legal and HR. | | | | X | | |

## II. ORGANIZATIONAL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization's information security infrastructure is supported by an:** | | | | | | |
| 2 | Enterprise-wide security steering committee. | | | | X | | |
| 2 | Information security representative from each business unit. | | | | X | | |
| 3 | Allocation of information security responsibilities. | | | | X | | |
| 2 | Information security advisor (for expert advice) or coordinator (to coordinate security knowledge sharing). | | | | X | | |
| 2 | Documented points of contact with law enforcement, standards setting organizations, and service providers for both incident response support and security advice. | | | | X | | |
| 2 | Autonomous oversight of information security policy implementation. | | | | X | | |
| 2 | Performing risk assessments before granting access to external parties. | | | | X | | |
| 2 | Management review and approval for the development or implementation of any new information technologies. | | | | X | | |
| | **Third party access is controlled in your organization by:** | | | | | | |
| 3 | Documenting the organization's security policy in the third-party contracts. | | X | | | | |
| 1 | Educating third-parties on the information classification program. | | X | | | | |

**II. ORGANIZATIONAL SECURITY (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Outsourcing is controlled in your organization by:** | | | | | | |
| 3 | Communicating legal requirements for protecting your organization's information and information technologies and services. | | X | | | | |
| 1 | Educating outsourcers on their liabilities in regards to the security of your organization's information, technologies and services. | | X | | | | |

## III. ASSET CLASSIFICATION & CONTROL

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization accounts for key information technology assets by:** | | | | | | |
| 1 | Recording the information and business ownership. | | X | | | | |
| | **Safeguarding information within your organization includes:** | | | | | | |
| 3 | A simple, effective guideline that indicates the degree of protection for each type of information asset. | | | | X | | |
| 3 | Handling and labeling procedures for physical media. | | | | X | | |

## IV. PERSONNEL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has policies and procedures in place that require:** | | | | | | |
| 2 | Information security roles and responsibilities included in all company job descriptions. | | | | X | | |
| 3 | All candidates for employment be adequately screened to ensure that their qualifications are accurate. | | X | | | | |
| 3 | All employees sign a confidentiality (non-disclosure) agreement to ensure that they understand their information handling responsibilities. | X | | | | | |
| | **An organizational-wide training program is in place for:** | | | | | | |
| 3 | Information security policy and procedure awareness and comprehension. | | | | X | | |
| 2 | Informing personnel of their legal responsibilities for security. | | X | | | | |
| 2 | Correct usage of information technologies including business applications. | X | | | | | |
| | **In response to a security incident or malfunction, a formal process exists in your organization that:** | | | | | | |
| 2 | Instructs employees on the correct method of handling security incidents. | | X | | | | |
| 1 | Instructs employees on the proper method for preserving the evidence necessary for forensic investigations. | | X | | | | |
| 3 | Disciplines employees who have violated security policies and procedures. | | | | X | | |

## V. PHYSICAL & ENVIRONMENTAL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Facilities are properly secured by:** | | | | | | |
| 3 | Adequately establishing and monitoring a physical perimeter. | X | | | | | |
| 3 | Logging and supervising physical entry by visitors. | X | | | | | |
| 2 | Taking precautions (including proper layout and site selection) to secure against natural or man-made disasters. | X | | | | | |
| 2 | Adequately controlling personnel or third parties working in secure areas. | X | | | | | |
| 2 | Controlling delivery and loading areas and if possible, isolating them from information processing facilities. | X | | | | | |
| 3 | Protecting equipment from power failures and other electrical anomalies. | X | | | | | |
| | **Equipment is properly secured by:** | | | | | | |
| 2 | Protecting power and telecommunications cabling from interception or damage. | X | | | | | |
| 3 | Correctly maintaining equipment to ensure its continued availability and integrity. | X | | | | | |
| 3 | Physically destroying storage devices containing sensitive information or securely overwriting sensitive data when disposing of those storage devices. | | | | X | | |

## V. PHYSICAL & ENVIRONMENTAL SECURITY (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization prevents the compromise or theft of information and information-processing facilities by requiring:** | | | | | | |
| 1 | A clear desk policy for papers and removable storage media, and a clear screen policy for information processing facilities. | | | | X | | |
| 2 | Equipment or information taken off site to be removed only with authorization, and proper logging is in place to control removal. | | | | X | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization ensures the correct and secure operation of information technologies by using:** | | | | | | |
| 3 | Documented standard operating procedures including processing information, scheduling, error handling, support, and recovery. | | | | X | | |
| 3 | A change management process. | | | | X | | |
| 2 | An incident management process. | | | | X | | |
| 3 | An enforceable segregation of duties policy. | | | | X | | |
| 3 | A separation between the development and operational (production) facilities. | X | | | | | |
| | **Your organization minimizes the risk that essential systems will fail by using acceptable:** | | | | | | |
| 3 | Capacity planning. | X | | | | | |
| | **Your organization protects the integrity and security of essential software and information by:** | | | | | | |
| 3 | Using a policy requiring compliance with software licenses. | X | | | | | |
| 2 | Using a policy for obtaining files and software from third parties. | X | | | | | |
| 3 | Installing and regularly updating anti-virus detection and repair software. | X | | | | | |
| 3 | Checking any files, electronic mail attachments or downloads of uncertain origin for viruses before use. | X | | | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization maintains the integrity and availability of essential information processing and communication services by:** | | | | | | |
| 3 | Implementing a backup and recovery process. | X | | | | | |
| 3 | Logging operator commands. | X | | | | | |
| 3 | Logging network and system faults. | X | | | | | |
| | **Your organization ensures the protection of networks and supporting infrastructure by:** | | | | | | |
| 3 | Establishing special controls to safeguard the confidentiality and integrity of data passing over public networks. | X | | | | | |
| 2 | Separating operational responsibility for the networks from the computer operations where possible. | X | | | | | |
| | **To prevent asset damage and business activity interruption, your organization's media should be controlled and physically protected by:** | | | | | | |
| 3 | Procedures for managing removable computer media such as CDs, disks, and printed reports. | | | | X | | |
| 3 | Securely storing system documentation. | | | | X | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization prevents loss, modification, or misuse of information exchanges between organizations by utilizing the appropriate:** | | | | | | |
| 2 | Agreements between organizations for the exchange of information. | | | | X | | |
| 2 | Security precautions for electronic commerce. | X | | | | | |
| 2 | Security precautions for electronic mail. | X | | | | | |
| 2 | Security precautions for electronic office systems such as voice mail, mobile communications, video, and postal services. | X | | | | | |
| 3 | Security precautions for publicly available systems such as web servers. | X | | | | | |

## VII. ACCESS CONTROL

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization controls access to sensitive information by:** | | | | | | |
| 1 | Documenting policy and business requirements for controlling access to each business application. | | | | X | | |
| 2 | Establishing access control rules that grant permissions to each group of users. | X | | | | | |
| | **Your organization prevents unauthorized access to information systems by:** | | | | | | |
| 2 | Using a formal user registration and de-registration procedure for granting access to all multi-user information systems. | X | | | | | |
| 2 | Controlling password allocation through a formal management process. | X | | | | | |
| | **To prevent unauthorized user access, your organization requires users to:** | | | | | | |
| 3 | Follow good security practices in the selection and use of passwords. | X | | | | | |
| 3 | Ensure that unattended equipment automatically logs users out or securely locks the system from unauthorized use. | X | | | | | |
| | **The protection of networked services is enforced by:** | | | | | | |
| 3 | Authenticating all users from external connections. | X | | | | | |
| 3 | Requiring authentication for an automatic connection to a network, such as in trust relationships between computers. | X | | | | | |

**VII. ACCESS CONTROL (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **All access to computer resources is restricted by operating system controls that:** | | | | | | |
| 1 | Authenticate connections using terminal identification when it is important to ensure logins occur only from specific locations and/or computers or terminals. | X | | | | | |
| 3 | Require a unique, non-descript identifier for all authorized users. | X | | | | | |
| 3 | Employ effective password management systems that ensure quality passwords. | X | | | | | |
| 2 | Restrict and log all use of system utilities. | X | | | | | |
| 2 | Permit time-of-day connection limits to high-risk or sensitive applications. | X | | | | | |
| | **All access and use of computer systems is monitored to detect unauthorized activities by:** | | | | | | |
| 3 | Recording all relevant security events in audit logs. | X | | | | | |
| 3 | Reviewing audit logs through an effective and routine process. | X | | | | | |
| 2 | Documenting and implementing procedures for monitoring the use of information technologies. | | | | X | | |
| 2 | Using a process to ensure that all system clocks are synchronized with an agreed standard. | | | | X | | |

**VII. ACCESS CONTROL (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has information security policies and procedures documented and implemented to control:** | | | | | | |
| 2 | The use of all mobile computing facilities including physical protection, access controls, cryptographic techniques, backups, and virus protection. | | | | X | | |
| 3 | All activities related to working remotely from a fixed site not located within your organization. | | | | X | | |

## VIII. SYSTEMS DEVELOPMENT AND MAINTENANCE

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization specifies security requirements and specifications that:** | | | | | | |
| 2 | Reflect the business value of the information assets involved. | X | | | | | |
| 2 | Follow a risk assessment and risk management process to determine the acceptable controls. | X | | | | | |
| | **Your organization uses cryptographic systems and techniques to protect the confidentiality, authenticity, or integrity of information by:** | | | | | | |
| 2 | Considering regulatory restrictions that may apply to the use of cryptographic algorithms in different parts of the world. | | | | X | | |
| 2 | Applying digital signatures to any form of legal or business document being processed electronically. | | | | X | | |
| 3 | Implementing a system for the management of cryptographic keys. | X | | | | | |
| | **System files are secured during IT projects and support activities by:** | | | | | | |
| 2 | Controlling program source libraries in the development process to restrict possible corruption or tampering. | X | | | | | |

**VIII. SYSTEMS DEVELOPMENT AND MAINTENANCE (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **In order to minimize the corruption of information systems, your organization controls the implementation of changes by:** | | | | | | |
| 3 | Using access controls to restrict the movement of programs and data from development into production. | X | | | | | |
| 2 | Testing the application system when a change in the operating system occurs to ensure that there is no adverse impact on operation or security. | X | | | | | |
| 2 | Conducting source code reviews to eliminate possible security vulnerabilities. | X | | | | | |

## IX. BUSINESS CONTINUITY MANAGEMENT

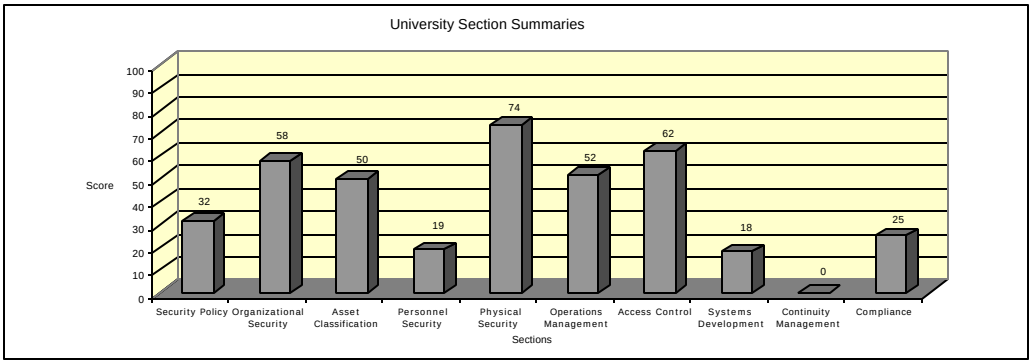
| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has a business continuity planning process in place that:** | | | | | | |
| 3 | Has produced a current, comprehensive, documented, and routinely-maintained business continuity plan for the entire organization. | | | | X | | |
| 2 | Requires the completion of a business impact analysis that identifies events and their associated risks. | | | | X | | |
| 2 | Requires a current prioritization of all business processes and supporting functions, including computer systems and applications. | | | | X | | |
| 2 | Ensures that the business continuity plan is routinely tested using effective techniques to assure that the plan is viable. | | | | X | | |

## X. COMPLIANCE

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has implemented policies and procedures to ensure compliance with legal requirements that specifically address the:** | | | | | | |
| 3 | Data protection and privacy of personal information. | X | | | | | |
| 3 | Acceptable use of information technologies. | | | | X | | |
| 2 | International usage or transport of cryptographic controls. | | | | X | | |
| | **Compliance procedures are in place that require the:** | | | | | | |
| 3 | Departmental managers to perform routine self-assessments to ensure that their areas comply with security policies and standards. | | | | X | | |
| 2 | Technical checking of information systems by independent experts for compliance with security standards and leading practices. | X | | | | | |
| | **Audit procedures are in place that require:** | | | | | | |
| 2 | Review of all operational systems to minimize the risk of business process disruptions. | | | | X | | |
| 2 | Restricted access to system audit tools to prevent misuse or compromise. | | | | X | | |

APPENDIX E

UNIVERSITY SURVEY RESULTS




*Source*: Security Management Index, Human Firewall Project, www.humanfirewall.org

## I. SECURITY POLICY

| Weighting | | Fully Implemente | Partially Implemente | Planned | Not Implemente d or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **The current information security policies within your organization:** | | | | | | |
| 3 | Define information security objectives and illustrate the importance of security. | | X | | | | |
| 3 | Provide a statement of management's intentions to support information security. | | | X | | | |
| 3 | Define general responsibilities for employees | | | X | | | |
| 3 | Reference other corporate documents. | | | | | X | |
| | **When reviewing, evaluating, and distributing security policies, your organization:** | | | | | | |
| 3 | Specifies a distinct information security owner who has the responsibility for update and maintenance of those policies. | | X | | | | |
| 3 | Requires a review by business owners, legal and HR. | | | X | | | |

## II. ORGANIZATIONAL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization's information security infrastructure is supported by an:** | | | | | | |
| 2 | Enterprise-wide security steering committee. | | X | | | | |
| 2 | Information security representative from each business unit. | | X | | | | |
| 3 | Allocation of information security responsibilities. | | X | | | | |
| 2 | Information security advisor (for expert advice) or coordinator (to coordinate security knowledge sharing). | | X | | | | |
| 2 | Documented points of contact with law enforcement, standards setting organizations, and service providers for both incident response support and security advice. | X | | | | | |
| 2 | Autonomous oversight of information security policy implementation. | | X | | | | |
| 2 | Performing risk assessments before granting access to external parties. | X | | | | | |
| 2 | Management review and approval for the development or implementation of any new information technologies. | | X | | | | |
| | **Third party access is controlled in your organization by:** | | | | | | |
| 3 | Documenting the organization's security policy in the third-party contracts. | | X | | | | |
| 1 | Educating third-parties on the information classification program. | | | X | | | |

**II. ORGANIZATIONAL SECURITY (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Outsourcing is controlled in your organization by:** | | | | | | |
| 3 | Communicating legal requirements for protecting your organization's information and information technologies and services. | | | | | X | |
| 1 | Educating outsourcers on their liabilities in regards to the security of your organization's information, technologies and services. | | | | | X | |

## III. ASSET CLASSIFICATION & CONTROL

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization accounts for key information technology assets by:** | | | | | | |
| 1 | Recording the information and business ownership. | | X | | | | |
| | **Safeguarding information within your organization includes:** | | | | | | |
| 3 | A simple, effective guideline that indicates the degree of protection for each type of information asset. | | X | | | | |
| 3 | Handling and labeling procedures for physical media. | | X | | | | |

## IV. PERSONNEL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has policies and procedures in place that require:** | | | | | | |
| 2 | Information security roles and responsibilities included in all company job descriptions. | | | X | | | |
| 3 | All candidates for employment be adequately screened to ensure that their qualifications are accurate. | | | | X | | |
| 3 | All employees sign a confidentiality (non-disclosure) agreement to ensure that they understand their information handling responsibilities. | | | | X | | |
| | **An organizational-wide training program is in place for:** | | | | | | |
| 3 | Information security policy and procedure awareness and comprehension. | | | X | | | |
| 2 | Informing personnel of their legal responsibilities for security. | | X | | | | |
| 2 | Correct usage of information technologies including business applications. | | | X | | | |
| | **In response to a security incident or malfunction, a formal process exists in your organization that:** | | | | | | |
| 2 | Instructs employees on the correct method of handling security incidents. | | X | | | | |
| 1 | Instructs employees on the proper method for preserving the evidence necessary for forensic investigations. | | X | | | | |
| 3 | Disciplines employees who have violated security policies and procedures. | | | | X | | |

## V. PHYSICAL & ENVIRONMENTAL SECURITY

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Facilities are properly secured by:** | | | | | | |
| 3 | Adequately establishing and monitoring a physical perimeter. | X | | | | | |
| 3 | Logging and supervising physical entry by visitors. | X | | | | | |
| 2 | Taking precautions (including proper layout and site selection) to secure against natural or man-made disasters. | | X | | | | |
| 2 | Adequately controlling personnel or third parties working in secure areas. | X | | | | | |
| 2 | Controlling delivery and loading areas and if possible, isolating them from information processing facilities. | | X | | | | |
| 3 | Protecting equipment from power failures and other electrical anomalies. | X | | | | | |
| | **Equipment is properly secured by:** | | | | | | |
| 2 | Protecting power and telecommunications cabling from interception or damage. | X | | | | | |
| 3 | Correctly maintaining equipment to ensure its continued availability and integrity. | | X | | | | |
| 3 | Physically destroying storage devices containing sensitive information or securely overwriting sensitive data when disposing of those storage devices. | | X | | | | |

**V. PHYSICAL & ENVIRONMENTAL SECURITY (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization prevents the compromise or theft of information and information-processing facilities by requiring:** | | | | | | |
| 1 | A clear desk policy for papers and removable storage media, and a clear screen policy for information processing facilities. | | | X | | | |
| 2 | Equipment or information taken off site to be removed only with authorization, and proper logging is in place to control removal. | | X | | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization ensures the correct and secure operation of information technologies by using:** | | | | | | |
| 3 | Documented standard operating procedures including processing information, scheduling, error handling, support, and recovery. | | | X | | | |
| 3 | A change management process. | | | | X | | |
| 2 | An incident management process. | | | | X | | |
| 3 | An enforceable segregation of duties policy. | | | | X | | |
| 3 | A separation between the development and operational (production) facilities. | | X | | | | |
| | **Your organization minimizes the risk that essential systems will fail by using acceptable:** | | | | | | |
| 3 | Capacity planning. | | X | | | | |
| | **Your organization protects the integrity and security of essential software and information by:** | | | | | | |
| 3 | Using a policy requiring compliance with software licenses. | X | | | | | |
| 2 | Using a policy for obtaining files and software from third parties. | | X | | | | |
| 3 | Installing and regularly updating anti-virus detection and repair software. | X | | | | | |
| 3 | Checking any files, electronic mail attachments or downloads of uncertain origin for viruses before use. | X | | | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization maintains the integrity and availability of essential information processing and communication services by:** | | | | | | |
| 3 | Implementing a backup and recovery process. | X | | | | | |
| 3 | Logging operator commands. | | X | | | | |
| 3 | Logging network and system faults. | X | | | | | |
| | **Your organization ensures the protection of networks and supporting infrastructure by:** | | | | | | |
| 3 | Establishing special controls to safeguard the confidentiality and integrity of data passing over public networks. | | | | | X | |
| 2 | Separating operational responsibility for the networks from the computer operations where possible. | | X | | | | |
| | **To prevent asset damage and business activity interruption, your organization's media should be controlled and physically protected by:** | | | | | | |
| 3 | Procedures for managing removable computer media such as CDs, disks, and printed reports. | | | X | | | |
| 3 | Securely storing system documentation. | | | X | | | |

## VI. COMMUNICATIONS AND OPERATIONS MANAGEMENT (continued)

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization prevents loss, modification, or misuse of information exchanges between organizations by utilizing the appropriate:** | | | | | | |
| 2 | Agreements between organizations for the exchange of information. | | X | | | | |
| 2 | Security precautions for electronic commerce. | | | | | X | |
| 2 | Security precautions for electronic mail. | | | | | X | |
| 2 | Security precautions for electronic office systems such as voice mail, mobile communications, video, and postal services. | | | | | X | |
| 3 | Security precautions for publicly available systems such as web servers. | | X | | | | |

## VII. ACCESS CONTROL

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization controls access to sensitive information by:** | | | | | | |
| 1 | Documenting policy and business requirements for controlling access to each business application. | | | | X | | |
| 2 | Establishing access control rules that grant permissions to each group of users. | | X | | | | |
| | **Your organization prevents unauthorized access to information systems by:** | | | | | | |
| 2 | Using a formal user registration and de-registration procedure for granting access to all multi-user information systems. | | X | | | | |
| 2 | Controlling password allocation through a formal management process. | X | | | | | |
| | **To prevent unauthorized user access, your organization requires users to:** | | | | | | |
| 3 | Follow good security practices in the selection and use of passwords. | | X | | | | |
| 3 | Ensure that unattended equipment automatically logs users out or securely locks the system from unauthorized use. | | X | | | | |
| | **The protection of networked services is enforced by:** | | | | | | |
| 3 | Authenticating all users from external connections. | X | | | | | |
| 3 | Requiring authentication for an automatic connection to a network, such as in trust relationships between computers. | X | | | | | |

**VII. ACCESS CONTROL (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **All access to computer resources is restricted by operating system controls that:** | | | | | | |
| 1 | Authenticate connections using terminal identification when it is important to ensure logins occur only from specific locations and/or computers or terminals. | | X | | | | |
| 3 | Require a unique, non-descript identifier for all authorized users. | X | | | | | |
| 3 | Employ effective password management systems that ensure quality passwords. | X | | | | | |
| 2 | Restrict and log all use of system utilities. | | X | | | | |
| 2 | Permit time-of-day connection limits to high-risk or sensitive applications. | | X | | | | |
| | **All access and use of computer systems is monitored to detect unauthorized activities by:** | | | | | | |
| 3 | Recording all relevant security events in audit logs. | | X | | | | |
| 3 | Reviewing audit logs through an effective and routine process. | | X | | | | |
| 2 | Documenting and implementing procedures for monitoring the use of information technologies. | | | | X | | |
| 2 | Using a process to ensure that all system clocks are synchronized with an agreed standard. | X | | | | | |

**VII. ACCESS CONTROL (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has information security policies and procedures documented and implemented to control:** | | | | | | |
| 2 | The use of all mobile computing facilities including physical protection, access controls, cryptographic techniques, backups, and virus protection. | | X | | | | |
| 3 | All activities related to working remotely from a fixed site not located within your organization. | | | | X | | |

## VIII. SYSTEMS DEVELOPMENT AND MAINTENANCE

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization specifies security requirements and specifications that:** | | | | | | |
| 2 | Reflect the business value of the information assets involved. | | | | X | | |
| 2 | Follow a risk assessment and risk management process to determine the acceptable controls. | | | | X | | |
| | **Your organization uses cryptographic systems and techniques to protect the confidentiality, authenticity, or integrity of information by:** | | | | | | |
| 2 | Considering regulatory restrictions that may apply to the use of cryptographic algorithms in different parts of the world. | | | | X | | |
| 2 | Applying digital signatures to any form of legal or business document being processed electronically. | | | | X | | |
| 3 | Implementing a system for the management of cryptographic keys. | | | | X | | |
| | **System files are secured during IT projects and support activities by:** | | | | | | |
| 2 | Controlling program source libraries in the development process to restrict possible corruption or tampering. | | X | | | | |

**VIII. SYSTEMS DEVELOPMENT AND MAINTENANCE (continued)**

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **In order to minimize the corruption of information systems, your organization controls the implementation of changes by:** | | | | | | |
| 3 | Using access controls to restrict the movement of programs and data from development into production. | | X | | | | |
| 2 | Testing the application system when a change in the operating system occurs to ensure that there is no adverse impact on operation or security. | | X | | | | |
| 2 | Conducting source code reviews to eliminate possible security vulnerabilities. | | | | X | | |

## IX. BUSINESS CONTINUITY MANAGEMENT

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has a business continuity planning process in place that:** | | | | | | |
| 3 | Has produced a current, comprehensive, documented, and routinely-maintained business continuity plan for the entire organization. | | | | X | | |
| 2 | Requires the completion of a business impact analysis that identifies events and their associated risks. | | | | X | | |
| 2 | Requires a current prioritization of all business processes and supporting functions, including computer systems and applications. | | | | X | | |
| 2 | Ensures that the business continuity plan is routinely tested using effective techniques to assure that the plan is viable. | | | | X | | |

## X. COMPLIANCE

| Weighting | | Fully Implemented | Partially Implemented | Planned | Not Implemented or Planned | Not Applicable | Answer at a Later Date |
|---|---|---|---|---|---|---|---|
| | **Your organization has implemented policies and procedures to ensure compliance with legal requirements that specifically address the:** | | | | | | |
| 3 | Data protection and privacy of personal information. | | | | | X | |
| 3 | Acceptable use of information technologies. | | | X | | | |
| 2 | International usage or transport of cryptographic controls. | | | | X | | |
| | **Compliance procedures are in place that require the:** | | | | | | |
| 3 | Departmental managers to perform routine self-assessments to ensure that their areas comply with security policies and standards. | | X | | | | |
| 2 | Technical checking of information systems by independent experts for compliance with security standards and leading practices. | | | | X | | |
| | **Audit procedures are in place that require:** | | | | | | |
| 2 | Review of all operational systems to minimize the risk of business process disruptions. | | | X | | | |
| 2 | Restricted access to system audit tools to prevent misuse or compromise. | | X | | | | |

REFERENCE LIST

Ackerman, Robert K. 2002. Government enlists industry for information security. *SIGNAL*, August, 17.

Adams, James. *The Next World War*. New York, NY: Simon & Schuster, 1998.

Applegate, Lynda M., F. Warren McFarlan, and James L. McKenney. *Corporate Information Systems Management*. Boston, MA: Irwin/McGraw-Hill, 1999.

Arquilla, John, and David Ronfeldt, eds. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND, 1997.

Ashworth, Rob. 2003. Information Assurance in Central Command. Conference Briefing, CENTCOM J6, Tampa Convention Center, Florida, 12 March.

Berry, Jonathon. "Defense in Depth: Preventing Going Hairless Over Wireless" [On-Line], (SANS Information Security Reading Room, April 17, 2002). Available from http://rr.sans.org/wireless/hairless.php; Internet.

Boyce, Joseph G., and Dan W. Jennings. *Information Assurance: Managing Organizational Security Risks*. Woburn, MA: Butterworth-Heinemann, 2002.

Browne, Herbert A. 2002. Let's bite the bullet and pay for information security. *SIGNAL*, August, 14.

Bunker, Robert J., *Five-Dimensional (Cyber) Warfighting: Can the Army After Next be Defeated Through Complex Concepts and Technologies?* Carlisle Barracks, PN: U.S. Army War College, 1998.

Daigle, Richard C. 2001. An Analysis of the Computer and Network Attack Taxonomy. Masters thesis, Air Force Institute of Technology.

Devost, Matthew G., Brian K. Houghton, and Neal A. Pollard. *Information Terrorism: Can You Trust Your Toaster?* [On-line]. (Science Application International Coorperation, 1996) Available from http://www.ndu.edu/inss/siws/ch3.html; Internet.

Doyle, James. *Handbook for IQP Advisors and Students*. [On-line]. Available from http://www.wpi.edu/Academics/Dpets/IGSD/IQPHbook/ch11e.html; Internet.

Dunlap, Charles. “How We Lost the High-Tech War of 2007” [On-Line], (The Weekly Standard, January 29, 1996). Available from http://www.weeklystandard.com/Content/Public/Articles/000/000/001/569nzbrd.asp; Internet.

Federal Bureau of Investigation. “About InfraGard” [On-Line], September 2002. Available from http://www.infraguard.net; Internet.

Fisher, Dennis. “Microsoft Security Under Fire” [On-Line], (eWeek, August 19, 2002). Available from http://www.eweek.com/article2/0,3959,476333,00.asp; Internet.

Ganger, Gregory R. and David F. Nagle. “Better Security via Smarter Devices” [On-Line], (Carnegie Mellon University, May 2001). Available from http://www.pdl.cmu.edu/PDL-FTP/Secure/hotos01_abs.html; Internet.

Gibson, Tim. “An Architecture for Flexible Multi-Security Domain Networks” [On-Line], (Security Symposium, February 2001). Available from http://www.cs.umbc.edu/~tgibso2/pubs/ndss2001/; Internet.

Hafner, Katie and Matthew Lyon. *Where Wizards Stay Up Late: The Origins of the Internet*. New York, NY: Simon & Schuster, 1996.

Hale, Richard. 2003. Cyber Perimeter Defense Improvements in DoD. Conference Briefing, Defense Information Systems Agency, Tampa Convention Center, Florida, 12 March.

Harney, Kerrie L. “Defense in Depth: From Risk Assessment to Self Assessment – A Dynamic Process” [On-Line], (Global Information Assurance Certification). Available from http://www.giac.org/GSEC_1400.php; Internet.

Hayes, Frank. “Hacker Lessons” [On-line], (Computerworld, August 16, 1999). Available from http://www.computerworld.com/news/1999/story/0,11280,36720,00.html; Internet.

Herrmann, Debra S. *A Practical Guide to Security Engineering and Information Assurance*. Boca Raton, FL: Auerbach Publishing, 2001.

Human Firewall Council, “Security Management Index” [On-Line] Available from http://www.humanfirewall.org; Internet.

Hurd, Bryan. 2002. Information and Computer Security Issues. Conference Briefing, American Society for Industrial Security, Overland Park, Kansas, 9 October.

Information Systems Security Association, “The Global Voice of Information Security” [On-Line] Available from http://www.issa.org; Internet.

Jones, Ian. “Mixing Qualitative and Quantitative Methods in Sports Fan Reasearch” [On-line], (The Qualitative Report, December 1997). Available from http://www.nova.edu/ssss/QR/QR3-4/jones.html; Internet.

Joint Staff Publication, Joint Pub 3-13, *Joint Doctrine for Information Operations*, Washington D.C., 1998.

Joint Staff Publication, *Information Assurance through Defense in Depth*, Washington D.C., 2000.

Kennedy, Kevin J., Bruce M. Lawlor, and Arne J. Nelson. *Grand Strategy for Information Age National Security*. Maxwell Air Force Base, AL: Air University Press, 1997.

Kent, Gary. Remarks given at the US Army Command and General Staff College, 4 Feb 03.

Kenyon, Henry S. 2002. Keeping malicious code at bay. *SIGNAL*, August, 29.

Kvale, Steinar. *InterViews: An Introduction to Qualitative Research Interviewing*. Newbury Park, CA: Sage Publications, 1997.

Landers, Jim. “As Threat of Cyber Attacks Grows, Security Specialists Blame Faulty Software” [On-Line], (NewsFactor Network, August 21, 2002). Available from http://www.newsfactor.com/perl/story/19104.html; Internet.

Larson, Eric V., and John E. Peters. *Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options*. Santa Monica, CA: RAND, 2001.

Lawlor, Maryann. 2002. National strategy tackles tough security issues. *SIGNAL*, August, 23.

Lyman, Jay. “Profile of the Perfect Security Guru” [On-Line], (NewsFactor Network, September 4, 2002). Available from http://www.newsfactor.com/perl/story/19299.html; Internet.

_____. “The Seven Deadly Security Sins” [On-Line], (NewsFactor Network, August 22, 2002). Available from http://www.newsfactor.com/perl/story/19116.html; Internet.

McClure, Stuart, Joel Scambray, and George Kurtz. *Hacking Exposed: Network Security Secrets and Solutions*. Berkeley, CA: Osborne/McGraw-Hill, 2001.

McKendrick, Joseph. 2002. Diverse groups share information assurance quandaries. *SIGNAL*, August, 41.

Microsoft. “Capacity Planning” [On-Line], (Microsoft Developer Network Library). Available from http://msdn.microsoft.com/library/default.asp?url=/library/en-us/comsrv2k/htm/cs_gs_planning_pqnj.asp; Internet.

Miller, Lawrence, and Peter Gregory. *CISSP for Dummies*. New York, NY: Wiley Publishing Inc., 2002.

Mitnick, Kevin D., and William L. Simon. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, IN: Wiley Publishing Inc., 2002.

National Defense Research Institute, 2000, *Advance Network Defense Research: Proceedings of a Workshop*, Santa Monica, CA.

National Security Agency, 2000, *Information Assurance Technical Framework* [On-Line], Fort Meade, MD: September 2002. Available from http://www.iatf.net/framework_docs/version-3_1/index.cfm; Internet.

Premo, Gregory J. 2003. Protecting the C4ISR Infrastructure in Challenging Environments. Conference Briefing, U.S. Army Training and Doctrine Command, Tampa Convention Center, Florida, 12 March.

Robinson, David W. “Defense in Depth: A Small University Takes Up the Challenge” [On-Line], (SANS Information Security Reading Room, April 7, 2002). Available from http://rr.sans.org/casestudies/small_univ.php; Internet.

Roeber, Rodney. 2003. WIN-T Information Briefing. Communications Seminar, Deputy TRADOC Systems Manager, US Army Command and General Staff Colleger, Kansas, 28 January.

Schiffman, Mike. *Hacker’s Challenge: Test Your Incident Response Skills Using 20 Scenarios*. Berkeley, CA: Osborne/McGraw-Hill, 2001.

Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World*. New York, NY: John Wiley & Sons, Inc., 2000.

Stewart, David W., *Secondary Research: Information Sources and Methods*. Newbury Park, CA: Sage Publications, 1984.

Summers, Rita A. *Secure Computing: Threats and Safeguards*. New York, NY: McGraw Hill Companies, Inc., 2000.

Sutherland, Ed. “Report: U.S. Computers Open to Hackers” [On-Line], (NewsFactor Network, August 3, 2001). Available from http://www.newsfactor.com/perl/story/12513.html; Internet.

Turabian, Kate L. 1996. *A Manual for Writer,* 6th ed. Chicago: University of Chicago Press.

VanMeter, Charlene. "Defense in Depth: A Primer" [On-Line], (SANS Information Security Reading Room, April 7, 2002). Available from http://www.san.org/rr/start/primer.php; Internet.

Verton, Dan. "White House cyber-security chief defines cyber-threat." [On-line]. (Computerworld, September 6, 2002) Available from http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801, 74033,00.html; Internet.

Voas, Jeffrey. "Protecting against What? The Achilles Heel of Information Assurance" [On-line], (IEEE Software, February 1999). Available from http://www.computer.org/software/so1999/s1028abs.htm; Internet.

Walk, Kerry. "How to Write a Comparative Analysis." [On-line]. (Writing Center at Harvard University, 1998) Available from http://www.fas.harvard.edu/~wricntr/documents/CompAnalysis.html; Internet.

Wired News. "Hacker Raises Stakes in DOD Attacks" [On-line], (Wired, march 4, 1998). Available from http://www.wired.com/news/technology/0,1282,10713,00.html; Internet.

Yin, Robert K., *Case Study Research: Design and Methods*. Newbury Park, CA: Sage Publications, 1989.

Yun, Ronald E., and Steven A. Vozzola. 2001. Network Defense-In-Depth: Evaluating Host-Based Intrusion Detection Systems. Master's Thesis, Naval Postgraduate School.

Web Development Company. 2003. Interview by author, 12 March, Tampa Convention Center, Florida.

U.S. Department of the Army, AR 380-5, *Department of the Army Information Security Program*: Washington, D.C.: Government Printing Office. September 2000.

U.S. Department of the Army, AR 380-19, *Information Systems Security*: Washington, D.C.: Government Printing Office. March 1998.

U.S. Department of the Army, FM 100-6, *Information Operations*: Washington, D.C.: Government Printing Office. August 1996.

U.S. Department of Defense. 2000. *Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510 (16 June 2000).* Washington, D.C.

U.S. General Accounting Office. 2002. *Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk.* Washington, D.C.: GPO.

United States. 2003. *National Strategy to Secure Cyberspace.* Washington, D.C.: GPO.

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

LtCol Richard W. Snyder, Chair
DJMO
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

LCDR Bob A. King
DJMO
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

LTC Kenneth D. Plowman
Consulting Faculty
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 6 June 2003

2. Thesis Author:

3. Thesis Title:

4. Thesis Committee Members: _____

Signatures: _____

_____

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

(A) B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

EXAMPLE

| Limitation Justification Statement | / | Chapter/Section | / | Page(s) |
|---|---|---|---|---|
| Direct Military Support (10) | / | Chapter 3 | / | 12 |
| Critical Technology (3) | / | Section 4 | / | 31 |
| Administrative Operational Use (7) | / | Chapter 2 | / | 13-32 |

Fill in limitation justification for your thesis below:

| Limitation Justification Statement | / | Chapter/Section | / | Page(s) |
|---|---|---|---|---|
| | / | | / | |
| | / | | / | |
| | / | | / | |
| | / | | / | |
| | / | | / | |

7. MMAS Thesis Author's Signature: _____

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).